



Panduan Referensi

AWS Pengelolaan Akun



AWS Pengelolaan Akun: Panduan Referensi

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Akun AWS?	1
Fitur dari sebuah Akun AWS	3
Apakah Anda yang pertama kali AWS pengguna?	3
AWS Layanan terkait	4
Menggunakan pengguna root	5
Support dan umpan balik	5
Lainnya AWS sumber daya	5
Memulai dengan akun Anda	7
Langkah 1: Buat akun Anda	8
Langkah 2: (Disarankan) Instal AWS CLI	10
Langkah 3: (Disarankan) Siapkan AWS MCP Server	10
Mengakses akun Anda	11
Rencanakan struktur tata kelola Anda	12
Manfaat Menggunakan Multiple Akun AWS	12
Mengelola beberapa Akun AWS	13
Kapan harus menggunakan AWS Organizations	14
Aktifkan akses terpercaya	15
Mengaktifkan akun admin yang didelegasikan	16
Batasi akses menggunakan SCPs	18
Kapan harus menggunakan AWS Control Tower	19
Memahami mode operasi API	20
Memberikan izin untuk memperbarui atribut akun	21
Konfigurasi akun Anda	24
Buat atau perbarui alias akun Anda	24
Aktifkan atau nonaktifkan Wilayah AWS di akun Anda	24
Referensi ketersediaan regional	27
Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah	29
Waktu pemrosesan dan batas permintaan	31
Mengaktifkan atau menonaktifkan Region untuk akun mandiri	31
Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda	33
Perbarui tagihan untuk Anda Akun AWS	36
Perbarui email pengguna root email	36
Perbarui email pengguna root untuk standalone Akun AWS atau akun manajemen	37
Perbarui email pengguna root untuk setiap Akun AWS di organisasi Anda	38

Perbarui kata sandi pengguna root	41
Perbarui Akun AWS name	42
Perbarui nama akun Anda untuk standalone Akun AWS	43
Perbarui nama akun Anda untuk apa pun Akun AWS di organisasi Anda	45
Perbarui kontak alternatif untuk Anda Akun AWS	46
Persyaratan nomor telepon dan alamat email	47
Perbarui kontak alternatif untuk mandiri Akun AWS	47
Perbarui kontak alternatif untuk apa pun Akun AWS di organisasi Anda	51
akun: kunci AlternateContactTypes konteks	55
Perbarui kontak utama untuk Anda Akun AWS	55
Persyaratan nomor telepon dan alamat email	56
Perbarui kontak utama untuk standalone Akun AWS atau akun manajemen	56
Perbarui kontak utama untuk apa pun AWS akun anggota di organisasi Anda	59
Lihat pengenal akun Anda	61
Temukan Anda Akun AWS ID	62
Temukan ID pengguna kanonik untuk Anda Akun AWS	65
Amankan akun Anda	68
Perlindungan data	69
AWS PrivateLink	70
Membuat Titik Akhir	70
Kebijakan Amazon VPC Endpoint	71
Kebijakan titik akhir	71
Identity and Access Management	72
Audiens	72
Mengautentikasi dengan identitas	73
Mengelola akses menggunakan kebijakan	74
AWS Manajemen Akun dan IAM	76
Identity-based contoh kebijakan	84
Menggunakan kebijakan berbasis identitas	87
Pemecahan masalah	90
AWS kebijakan terkelola	92
AWSAccountManagementReadOnlyAccess	93
AWSAccountManagementFullAccess	94
Pembaruan kebijakan	95
Validasi kepatuhan	95
Ketahanan	96

Keamanan infrastruktur	97
Pantau akun Anda	98
CloudTrail log	98
Informasi Manajemen Akun di CloudTrail	99
Memahami entri log Manajemen Akun	100
Memantau acara Manajemen Akun dengan EventBridge	103
Acara Manajemen Akun	103
Memecahkan masalah akun Anda	106
Masalah pembuatan akun	106
Masalah penutupan akun	107
Saya tidak tahu cara menghapus atau membatalkan akun saya	107
Saya tidak melihat tombol Tutup akun di halaman Akun	107
Saya menutup akun saya tetapi masih belum menerima konfirmasi email	108
Saya menerima kesalahan <code>ConstraintViolationException</code> saat mencoba menutup akun saya	108
Saya menerima kesalahan <code>"CLOSE_ACCOUNT_QUOTA_EXCEEDED"</code> saat mencoba menutup akun anggota	108
Apakah saya perlu menghapus AWS organisasi saya sebelum menutup akun manajemen?	109
Masalah lainnya	109
Saya perlu mengganti kartu kredit untuk saya Akun AWS	109
Saya perlu melaporkan penipuan Akun AWS aktivitas	109
Aku harus menutup Akun AWS	110
Tutup akun Anda	111
Apa yang perlu Anda ketahui sebelum menutup akun Anda	111
Cara menutup akun Anda	113
Apa yang diharapkan setelah Anda menutup akun Anda	116
Post-closure periode	116
Membuka kembali Anda Akun AWS	117
Referensi API	118
Tindakan	120
AcceptPrimaryEmailUpdate	122
DeleteAlternateContact	127
DisableRegion	132
EnableRegion	136
GetAccountInformation	140

GetAlternateContact	146
GetContactInformation	152
GetGovCloudAccountInformation	156
GetPrimaryEmail	162
GetRegionOptStatus	166
ListRegions	170
PutAccountName	175
PutAlternateContact	180
PutContactInformation	186
StartPrimaryEmailUpdate	190
Tindakan terkait	193
CreateAccount	194
CreateGovCloudAccount	194
DescribeAccount	194
Tipe Data	194
AlternateContact	196
ContactInformation	198
Region	202
ValidationExceptionField	203
Parameter Umum	203
Jenis Kesalahan Umum	205
Membuat permintaan Kueri HTTP	208
Titik akhir	209
HTTPS diperlukan	209
Menandatangani permintaan API Manajemen AWS Akun	209
Kuota	211
Kelola akun di India	213
Buat sebuah Akun AWS dengan AWS India	213
Kelola informasi verifikasi pelanggan Anda	216
Periksa status verifikasi pelanggan Anda	216
Buat informasi verifikasi pelanggan Anda	216
Mengedit informasi verifikasi pelanggan Anda	217
Dokumen India yang diterima untuk verifikasi pelanggan	218
Kelola Anda AWS Akun India	219
Riwayat dokumen	220
.....	ccxxiii

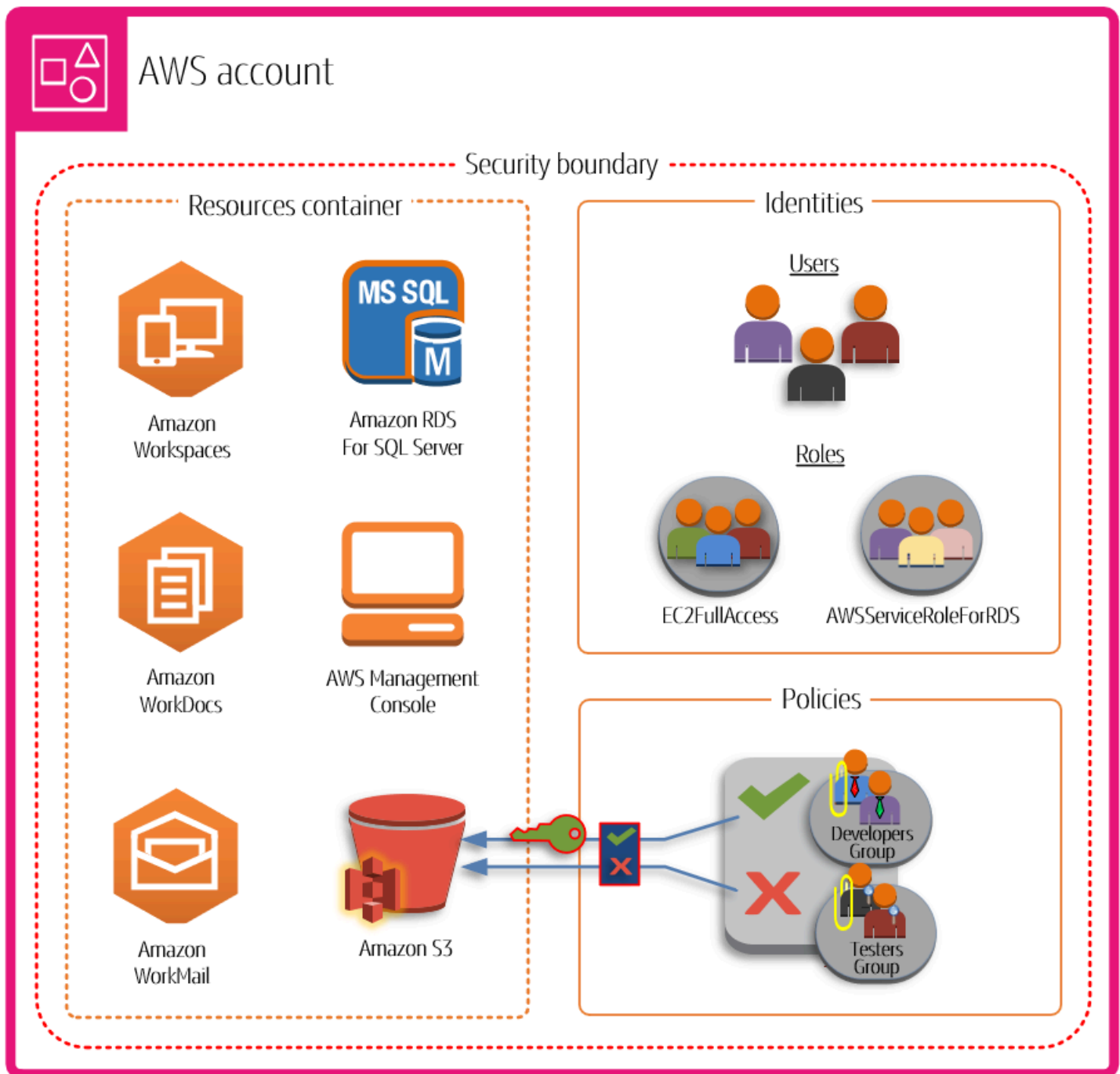
Apa itu Akun AWS?

An Akun AWS mewakili hubungan bisnis formal yang Anda bangun dengan AWS. Anda membuat dan mengelola AWS sumber daya Anda di Akun AWS, dan akun Anda menyediakan kemampuan manajemen identitas untuk akses dan penagihan. Masing-masing Akun AWS memiliki ID unik yang membedakannya dari yang lain Akun AWS.

Sumber daya dan data cloud Anda terkandung dalam file Akun AWS. Akun bertindak sebagai batas isolasi identitas dan manajemen akses. Ketika Anda perlu berbagi sumber daya dan data antara dua akun, Anda harus secara eksplisit mengizinkan akses ini. Secara default, tidak ada akses yang diizinkan antar akun. Misalnya, jika Anda menetapkan akun yang berbeda untuk memuat sumber daya dan data produksi dan non-produksi Anda, akses tidak diperbolehkan antara lingkungan tersebut secara default.

Akun AWS juga merupakan bagian mendasar dari mengakses AWS layanan. Seperti yang ditunjukkan dalam ilustrasi berikut, Akun AWS melayani dua fungsi utama:

- **Kontainer sumber daya** — An Akun AWS adalah wadah dasar untuk semua AWS sumber daya yang Anda buat sebagai AWS pelanggan. Misalnya, bucket Amazon Simple Storage Service (Amazon S3), database Amazon Relational Database Service (Amazon RDS), dan instans Amazon Elastic Compute Cloud (Amazon EC2) adalah semua sumber daya. Setiap sumber daya diidentifikasi secara unik oleh Nama Sumber Daya Amazon (ARN) yang menyertakan ID akun akun yang berisi, atau memiliki, sumber daya.
- **Batas keamanan** — An juga Akun AWS merupakan batas keamanan dasar untuk sumber daya Anda. AWS Sumber daya yang Anda buat di akun tersedia bagi pengguna yang memiliki kredensi untuk akun Anda. Di antara sumber daya utama yang dapat Anda buat di akun Anda adalah identitas, seperti pengguna dan peran. Identitas memiliki kredensi yang dapat digunakan seseorang untuk masuk (mengautentikasi). AWS Identitas juga memiliki kebijakan izin yang menentukan apa yang dapat dilakukan pengguna (otorisasi) dengan sumber daya di akun.



Menggunakan multiple Akun AWS adalah praktik terbaik untuk menskalakan lingkungan Anda, karena menyediakan batas penagihan alami untuk biaya, mengisolasi sumber daya untuk keamanan, memberikan fleksibilitas bagi individu dan tim, selain dapat beradaptasi untuk proses bisnis baru. Untuk informasi selengkapnya, lihat [Manfaat Menggunakan Multiple Akun AWS](#).

Fitur dari sebuah Akun AWS

Akun AWS termasuk fitur inti berikut:

- **Memantau dan mengendalikan biaya** — Akun adalah sarana default dimana AWS biaya dialokasikan. Karena fakta ini, menggunakan akun yang berbeda untuk unit bisnis dan kelompok beban kerja yang berbeda dapat membantu Anda melacak, mengontrol, memperkirakan, menganggarkan, dan melaporkan pengeluaran cloud Anda dengan lebih mudah. Selain pelaporan biaya di tingkat akun, AWS juga memiliki dukungan bawaan untuk mengkonsolidasikan dan melaporkan biaya di seluruh rangkaian akun Anda jika Anda memilih untuk digunakan AWS Organizations di beberapa titik. Anda juga dapat menggunakan AWS Service Quotas untuk membantu melindungi Anda dari penyediaan AWS sumber daya yang berlebihan dan tindakan berbahaya yang secara dramatis dapat memengaruhi biaya Anda. AWS
- **Unit isolasi** — An Akun AWS menyediakan batasan keamanan, akses, dan penagihan untuk AWS sumber daya Anda yang dapat membantu Anda mencapai otonomi dan isolasi sumber daya. Secara desain, semua sumber daya yang disediakan dalam akun secara logis diisolasi dari sumber daya yang disediakan di akun lain, bahkan di dalam lingkungan Anda sendiri. AWS Batas isolasi ini memberi Anda cara untuk membatasi risiko masalah terkait aplikasi, kesalahan konfigurasi, atau tindakan jahat. Jika masalah terjadi dalam satu akun, dampak terhadap beban kerja yang terdapat di akun lain dapat dikurangi atau dihilangkan.
- **Cerminkan beban kerja bisnis Anda** — Gunakan beberapa akun untuk mengelompokkan beban kerja dengan tujuan bisnis yang sama di akun yang berbeda. Akibatnya, Anda dapat menyelaraskan kepemilikan dan pengambilan keputusan dengan akun tersebut dan menghindari dependensi dan konflik dengan bagaimana beban kerja di akun lain diamankan dan dikelola. Tergantung pada model bisnis Anda secara keseluruhan, Anda dapat memilih untuk mengisolasi unit bisnis atau anak perusahaan yang berbeda dalam akun yang berbeda. Pendekatan ini juga dapat memudahkan divestasi unit-unit tersebut dari waktu ke waktu.

Apakah Anda yang pertama kali AWS pengguna?

Jika Anda adalah pengguna pertama kali AWS, langkah pertama Anda adalah mendaftar untuk Akun AWS Saat Anda mendaftar, AWS buat akun dengan detail yang Anda berikan dan berikan akun kepada Anda. Setelah Anda membuat Akun AWS, masuk sebagai [pengguna root](#), aktifkan otentikasi multi-faktor (MFA) untuk pengguna root, dan tetapkan akses administratif ke pengguna.

Untuk petunjuk langkah demi langkah tentang cara mengatur akun baru, lihat [Memulai dengan Akun AWS](#).

AWS Layanan terkait

Akun AWS bekerja dengan mulus dengan layanan berikut:

- IAM

Anda Akun AWS terintegrasi erat dengan AWS Identity and Access Management (IAM). Anda dapat menggunakan IAM dengan akun Anda untuk memastikan bahwa orang lain yang bekerja di akun Anda memiliki akses sebanyak yang mereka butuhkan untuk menyelesaikan pekerjaan mereka. Anda juga menggunakan IAM untuk mengontrol akses ke semua sumber AWS daya Anda, tidak hanya informasi spesifik akun. Penting bagi Anda untuk membiasakan diri dengan konsep utama dan praktik terbaik IAM sebelum Anda terlalu jauh dengan menyiapkan struktur Anda Akun AWS. Untuk informasi selengkapnya tentang administrator, lihat [Praktik terbaik keamanan di IAM](#) di dalam Panduan Pengguna IAM.

- AWS Organizations

Jika perusahaan Anda besar atau cenderung tumbuh, Anda mungkin ingin membuat beberapa AWS akun yang mencerminkan struktur spesifik perusahaan Anda. AWS Organizations menyediakan infrastruktur dan kemampuan yang mendasari bagi Anda untuk membangun dan mengelola lingkungan multi-akun Anda. Anda dapat menggabungkan akun yang ada ke dalam organisasi yang memungkinkan Anda mengelola akun secara terpusat. Anda dapat membuat akun yang secara otomatis menjadi bagian dari organisasi Anda, dan Anda dapat mengundang akun lain untuk bergabung dengan organisasi Anda. Anda juga dapat melampirkan kebijakan yang memengaruhi sebagian atau semua akun Anda. Untuk informasi selengkapnya, lihat [Kapan harus menggunakan AWS Organizations](#).

- AWS Control Tower

AWS Control Tower menyediakan cara yang disederhanakan untuk mengatur dan mengatur lingkungan multi-akun AWS yang aman. AWS Control Tower mengotomatiskan pembuatan lingkungan multi-akun Anda menggunakan AWS Organizations, membuat instance satu set akun awal dan dengan beberapa pagar pembatas dan konfigurasi default untuk lingkungan. Anda dapat menggunakan AWS Control Tower untuk menyediakan yang baru Akun AWS dalam beberapa langkah sambil memastikan bahwa akun sesuai dengan kebijakan organisasi Anda. Lihat informasi yang lebih lengkap di [Kapan harus menggunakan AWS Control Tower](#).

Menggunakan Pengguna root akun AWS

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Untuk menghindari penggunaan pengguna root untuk tugas sehari-hari, pelajari cara [mengatur pengguna administratif AWS IAM Identity Center](#). Untuk rekomendasi keamanan pengguna root tambahan, lihat [Praktik terbaik pengguna Root untuk Anda Akun AWS](#).

Important

Siapa pun yang memiliki kredensial pengguna root untuk Anda Akun AWS memiliki akses tidak terbatas ke semua sumber daya di akun Anda, termasuk informasi penagihan.

Anda dapat [mengubah](#), atau [mengatur ulang kata sandi pengguna root](#), dan [membuat](#), atau [menghapus kunci akses](#) (kunci akses IDs dan kunci akses rahasia) untuk pengguna root Anda. Untuk bantuan saat masuk menggunakan pengguna root, lihat [Masuk ke pengguna root Konsol Manajemen AWS sebagai pengguna root](#) di Panduan Pengguna AWS Masuk.

Support untuk AWS Pengelolaan Akun

Anda dapat memposting umpan balik dan pertanyaan menggunakan [forum dukungan Manajemen AWS Akun](#). Untuk informasi umum tentang AWS forum, lihat [AWS re:Post](#).

Jika Anda tidak dapat menemukan jawaban yang Anda cari AWS re:Post, Anda dapat membuat akun atau kasus dukungan terkait penagihan menggunakan Konsol Manajemen AWS Untuk informasi selengkapnya, lihat [Contoh: Membuat kasus dukungan untuk akun dan penagihan](#).

Lainnya AWS sumber daya

- [AWS Pelatihan dan Kursus](#) - Tautan ke kursus berbasis peran dan khusus serta laboratorium mandiri untuk membantu mempertajam AWS keterampilan Anda dan mendapatkan pengalaman praktis.

- [AWS Alat Pengembang](#) — Tautan ke alat dan sumber daya pengembang yang menyediakan dokumentasi, contoh kode, catatan rilis, dan informasi lainnya untuk membantu Anda membangun aplikasi inovatif AWS.
- [AWS Dukungan Center](#) — Hub untuk membuat dan mengelola kasus AWS Support Anda. Juga mencakup tautan ke sumber daya yang bermanfaat lainnya, seperti forum, Pertanyaan Umum teknis, status kesehatan layanan, dan AWS Trusted Advisor.
- [AWS Support](#) — Halaman web utama untuk informasi tentang AWS Support, saluran dukungan respons cepat satu-satu untuk membantu Anda membangun dan menjalankan aplikasi di cloud.
- [Hubungi Kami](#) — Titik kontak pusat untuk pertanyaan tentang AWS penagihan, akun, acara, penyalahgunaan, dan masalah lainnya.
- [AWS Ketentuan Situs](#) — Informasi terperinci tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; dan topik lainnya.

Memulai dengan Akun AWS

Jika Anda baru mengenal AWS, Anda harus mendaftar untuk Akun AWS. Ketika Anda melakukannya, AWS akan membuat akun menggunakan detail yang Anda berikan dan menetapkannya kepada Anda.

Untuk mendaftar Akun AWS, Anda harus memberikan informasi berikut:

- **Alamat email pengguna root** Alamat — Alamat email digunakan sebagai nama masuk untuk [pengguna root](#) dan diperlukan untuk pemulihan akun. Anda harus dapat menerima pesan email yang dikirim ke alamat ini. Sebelum Anda dapat melakukan tugas-tugas tertentu, Anda harus memverifikasi bahwa Anda memiliki akses ke email yang dikirim ke alamat ini.
- **AWS Nama akun** — Nama akun muncul di beberapa tempat, seperti pada faktur Anda, dan di konsol seperti dasbor Billing and Cost Management dan konsol. AWS Organizations Kami menyarankan Anda menggunakan cara standar untuk memberi nama akun Anda sehingga Anda dapat memberikan nama akun Anda yang mudah dikenali. Untuk akun perusahaan, pertimbangkan untuk menggunakan standar penamaan seperti organisasi - tujuan - lingkungan (misalnya, AnyCompany- audit - prod). Untuk akun pribadi, pertimbangkan untuk menggunakan standar penamaan seperti nama depan - nama belakang - tujuan (misalnya, paulo-santos-testaccount).
- **Alamat** - Jika kontak dan alamat penagihan Anda berada di India, perjanjian pengguna untuk akun Anda adalah dengan Amazon Web Services India Private Limited (AWS India), AWS penjual lokal di India. Anda harus memberikan CVV Anda sebagai bagian dari proses verifikasi. Anda mungkin juga harus memasukkan kata sandi satu kali, tergantung pada bank Anda. AWS India membebankan metode pembayaran Anda 2 INR sebagai bagian dari proses verifikasi. AWS India mengembalikan 2 INR setelah verifikasi selesai.
- **Nomor telepon** — Nomor ini digunakan untuk tujuan verifikasi identitas dan untuk mengonfirmasi kepemilikan akun Anda. Anda harus dapat menerima panggilan dan pesan SMS di nomor telepon ini.

Important

Jika akun ini untuk bisnis, gunakan nomor telepon perusahaan sehingga perusahaan Anda dapat mempertahankan akses ke Akun AWS bahkan ketika seorang karyawan mengubah posisi atau meninggalkan perusahaan.

Langkah 1: Buat akun Anda

Instruksi ini untuk membuat Akun AWS bagian luar India. Untuk membuat akun di India, lihat [Buat sebuah Akun AWS dengan AWS India](#). Untuk membuat akun yang merupakan bagian dari organisasi yang dikelola oleh AWS Organizations, lihat [Membuat akun anggota di organisasi](#) dalam Panduan AWS Organizations Pengguna.

Konsol Manajemen AWS

Untuk membuat Akun AWS

1. Buka AWS halaman [Daftar untuk](#).
2. Masukkan alamat email pengguna root dan Akun AWS nama, lalu pilih Verifikasi alamat email. Ini mengirimkan kode verifikasi ke alamat email Anda.

Important

Jika akun ini untuk bisnis, gunakan daftar distribusi perusahaan yang aman (misalnya, `it.admins@example.com`) sehingga perusahaan Anda dapat mempertahankan akses ke Akun AWS bahkan ketika seorang karyawan mengubah posisi atau meninggalkan perusahaan. Karena alamat email dapat digunakan untuk mengatur ulang kredensi pengguna root akun, lindungi akses ke daftar distribusi atau alamat ini.

3. Masukkan kode verifikasi Anda, lalu pilih Verifikasi.
4. Masukkan kata sandi yang kuat untuk pengguna root Anda, konfirmasi, lalu pilih Lanjutkan. AWS mengharuskan kata sandi Anda memenuhi ketentuan berikut:
 - Itu harus memiliki minimal 8 karakter dan maksimal 128 karakter.
 - Ini harus mencakup minimal tiga dari campuran tipe karakter berikut: huruf besar, huruf kecil, angka, dan `! @ # $ % ^ & * () < > [] { } | _ + =` simbol.
 - Itu tidak boleh identik dengan Akun AWS nama atau alamat email Anda.
5. Pilih paket akun Anda. Untuk informasi selengkapnya, lihat [Paket Tingkat Gratis](#).
6. Masukkan informasi kontak Anda, lalu baca dan terima [Perjanjian AWS Pelanggan](#). Pastikan Anda memahami persyaratan sebelum menerima.

⚠ Important

Jika akun ini untuk bisnis, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan daripada nomor untuk telepon pribadi. Mengkonfigurasi pengguna root akun dengan alamat email individual atau nomor telepon pribadi dapat membuat akun Anda tidak aman.

7. Masukkan informasi penagihan Anda. Jika Anda ingin menggunakan alamat penagihan yang berbeda untuk informasi AWS penagihan Anda, pilih Gunakan alamat baru.

Anda tidak dapat melanjutkan proses pendaftaran sampai Anda menambahkan metode pembayaran yang valid.

8. Anda mungkin perlu mengonfirmasi identitas Anda:
 - a. Untuk kode Negara atau wilayah, masukkan nomor telepon yang dapat dihubungi dalam beberapa menit ke depan.
 - b. Untuk nomor Telepon, masukkan nomor telepon yang dapat dihubungi dalam beberapa menit ke depan.
 - c. Pilih Kirim SMS.
 - d. Ketika sistem otomatis menghubungi Anda, masukkan kode yang Anda terima dan kemudian pilih Lanjutkan.
9. Pilih salah satu AWS Dukungan paket yang tersedia. Untuk penjelasan tentang paket Support yang tersedia dan manfaatnya, lihat [Membandingkan Dukungan paket](#).
10. Pilih Daftar lengkap. Halaman konfirmasi muncul yang menunjukkan bahwa akun Anda sedang diaktifkan.
11. Periksa folder email dan spam Anda untuk pesan email yang mengonfirmasi akun Anda telah diaktifkan. Aktivasi biasanya memakan waktu beberapa menit tetapi terkadang bisa memakan waktu hingga 24 jam.
12. Setelah menerima pesan aktivasi, Anda dapat masuk ke untuk [Konsol Manajemen AWS](#) mulai menggunakan Layanan AWS. Untuk informasi umum tentang cara mengelola setelan akun, lihat [Konfigurasi Akun AWS](#).

Untuk beberapa yang Akun AWS dikelola melalui AWS Organizations, tetapkan akses administratif ke pengguna administratif di Pusat Identitas IAM. Untuk petunjuk, lihat [Mengatur](#)

[Akun AWS akses untuk pengguna administratif Pusat Identitas IAM di Panduan Pengguna Pusat Identitas IAM.](#)

AWS CLI & SDKs

Anda dapat membuat akun anggota di organisasi yang dikelola AWS Organizations dengan menjalankan [CreateAccount](#) operasi saat masuk ke akun manajemen organisasi.

Anda tidak dapat membuat mandiri Akun AWS di luar organisasi dengan menggunakan operasi AWS Command Line Interface (AWS CLI) atau AWS API.

Langkah 2: (Disarankan) Instal AWS CLI

Instal AWS CLI dengan mengikuti petunjuk di [Instalasi AWS CLI](#). Anda memerlukan versi 2.32.0 atau yang lebih baru.

Anda dapat menggunakan AWS CLI untuk memiliki agen mengelola AWS sumber daya atas nama Anda.

Setelah Anda menginstal AWS CLI, gunakan perintah berikut untuk masuk secara terprogram:

```
aws login
```

Ini secara otomatis memutar kredensi Anda setiap 15 menit, menjaga sesi Anda tetap valid hingga 12 jam tanpa intervensi manual.

Gunakan perintah berikut untuk memverifikasi kredensial Anda berfungsi:

```
aws sts get-caller-identity
```

Untuk informasi selengkapnya tentang mengakses Anda Akun AWS, lihat [Mengakses Anda Akun AWS](#).

Langkah 3: (Disarankan) Siapkan AWS MCP Server

AWS MCP Server adalah server terkelola yang memberikan akses agen AWS melalui Model Context Protocol (MCP). Agen dapat mencari AWS dokumentasi dan mengambil informasi layanan tanpa otentikasi. Untuk menjalankan panggilan AWS API, jalankan skrip Python di lingkungan kotak pasir,

atau ikuti keterampilan yang dikuratori, agen mengautentikasi melalui kredensial IAM Anda yang ada. Untuk informasi selengkapnya, lihat [Apa itu Toolkit AWS Agen?](#)

Mengakses Anda Akun AWS

Anda dapat mengakses Anda Akun AWS dengan salah satu cara berikut:

Konsol Manajemen AWS

[Konsol Manajemen AWS Ini adalah antarmuka berbasis browser yang dapat Anda gunakan untuk mengelola Akun AWS pengaturan dan sumber daya Anda AWS .](#)

AWS Alat Baris Perintah

Dengan alat baris AWS perintah, Anda dapat mengeluarkan perintah di baris perintah sistem Anda untuk melakukan Akun AWS dan AWS tugas. Dengan menggunakan baris perintah dapat lebih cepat dan lebih nyaman dibandingkan menggunakan konsol tersebut. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan AWS tugas. AWS menyediakan dua set alat baris perintah:

- [AWS Command Line Interface](#)(AWS CLI). Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat [Panduan AWS Command Line Interface Pengguna](#).
- [AWS Tools for Windows PowerShell](#). Untuk informasi tentang menginstal dan menggunakan Alat untuk Windows PowerShell, lihat [Panduan Alat AWS untuk PowerShell Pengguna](#).

AWS SDKs

Ini AWS SDKs terdiri dari perpustakaan dan kode sampel untuk berbagai bahasa pemrograman dan platform (misalnya, Java, Python, Ruby, .NET, iOS, dan Android). SDKs Menangani tugas-tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba ulang permintaan secara otomatis. Untuk informasi selengkapnya tentang AWS SDKs, termasuk cara mengunduh dan menginstalnya, lihat [Alat untuk Amazon Web Services](#).

AWS Manajemen Akun HTTPS Query API

AWS Account Management HTTPS Query API memberi Anda akses terprogram ke Akun AWS dan AWS. API Kueri HTTPS memungkinkan Anda menerbitkan permintaan HTTPS secara langsung ke layanan. Saat Anda menggunakan HTTPS API, Anda harus menyertakan kode untuk menandatangani permintaan secara digital menggunakan kredensial Anda. Untuk informasi selengkapnya, lihat [Memanggil API dengan membuat permintaan Kueri HTTP](#).

Rencanakan struktur Akun AWS tata kelola Anda

Meskipun Anda mungkin telah memulai AWS perjalanan dengan satu akun, AWS menyarankan agar Anda menyiapkan beberapa akun karena beban kerja Anda bertambah besar dan kompleksitas. Apakah Anda adalah bisnis menengah atau perusahaan besar, Anda akan ingin membuat rencana struktur tata kelola yang akan memastikan data dan kebutuhan beban kerja Anda terpenuhi.

Bagian ini mencakup manfaat dan layanan tata kelola yang tersedia AWS untuk membantu mengaktifkan struktur tata kelola multi-akun.

Topik

- [Manfaat Menggunakan Multiple Akun AWS](#)
- [Kapan harus menggunakan AWS Organizations](#)
- [Kapan harus menggunakan AWS Control Tower](#)
- [Memahami mode operasi API](#)

Manfaat Menggunakan Multiple Akun AWS

Akun AWS membentuk batas keamanan dasar di AWS Cloud Mereka berfungsi sebagai wadah untuk sumber daya, menyediakan lapisan isolasi kritis yang penting untuk menciptakan lingkungan yang aman dan diatur dengan baik. Untuk informasi selengkapnya, lihat [Apa itu Akun AWS?](#).

Memisahkan sumber daya Anda menjadi terpisah Akun AWS membantu Anda mendukung prinsip-prinsip berikut di lingkungan cloud Anda:

- Kontrol keamanan — Aplikasi yang berbeda dapat memiliki profil keamanan yang berbeda, memerlukan kebijakan dan mekanisme kontrol yang berbeda di sekitarnya. Misalnya, jauh lebih mudah untuk berbicara dengan auditor dan dapat menunjuk ke satu Akun AWS yang menampung semua elemen beban kerja Anda yang tunduk pada Standar Keamanan [Industri Kartu Pembayaran \(PCI\)](#).
- Isolasi — An Akun AWS adalah unit perlindungan keamanan. Potensi risiko dan ancaman keamanan harus terkandung dalam sebuah Akun AWS tanpa mempengaruhi orang lain. Mungkin ada kebutuhan keamanan yang berbeda karena tim yang berbeda atau profil keamanan yang berbeda.

- Banyak tim — Tim yang berbeda memiliki tanggung jawab dan kebutuhan sumber daya yang berbeda. Anda dapat mencegah tim mengganggu satu sama lain dengan memindahkan mereka untuk memisahkan Akun AWS.
- Isolasi data — Selain mengisolasi tim, penting untuk mengisolasi penyimpanan data ke akun. Ini dapat membantu membatasi jumlah orang yang dapat mengakses dan mengelola penyimpanan data tersebut. Ini membantu menahan paparan data yang sangat pribadi dan oleh karena itu dapat membantu mematuhi [Peraturan Perlindungan Data Umum \(GDPR\) Uni Eropa](#).
- Proses bisnis — Unit bisnis atau produk yang berbeda mungkin memiliki tujuan dan proses yang sama sekali berbeda. Dengan beberapa Akun AWS, Anda dapat mendukung kebutuhan spesifik unit bisnis.
- Penagihan — Akun adalah satu-satunya cara yang benar untuk memisahkan item pada tingkat penagihan. Beberapa akun membantu memisahkan item pada tingkat penagihan di seluruh unit bisnis, tim fungsional, atau pengguna individu. Anda masih bisa mendapatkan semua tagihan Anda dikonsolidasikan ke satu pembayar (menggunakan AWS Organizations dan menggabungkan tagihan) sambil memisahkan item baris. Akun AWS
- Alokasi kuota — kuota AWS layanan diberlakukan secara terpisah untuk masing-masing. Akun AWS Memisahkan beban kerja menjadi berbeda Akun AWS mencegah mereka dari mengkonsumsi kuota untuk satu sama lain.

Semua rekomendasi dan prosedur yang dijelaskan dalam dokumen ini sesuai dengan Kerangka Kerja [AWS Well-Architected](#). Kerangka kerja ini dimaksudkan untuk membantu Anda merancang infrastruktur cloud yang fleksibel, tangguh, dan terukur. Bahkan ketika Anda memulai dari yang kecil, kami sarankan Anda melanjutkan sesuai dengan panduan ini dalam kerangka kerja. Melakukan hal itu dapat membantu Anda meningkatkan skala lingkungan Anda dengan aman dan tanpa memengaruhi operasi Anda yang sedang berlangsung saat Anda tumbuh.

Mengelola beberapa Akun AWS

Sebelum Anda mulai menambahkan beberapa akun, Anda akan ingin mengembangkan rencana untuk mengelolanya. Untuk itu, kami sarankan Anda menggunakan [AWS Organizations](#), yang merupakan AWS layanan gratis untuk mengelola semua yang ada Akun AWS di organisasi Anda.

AWS juga menawarkan AWS Control Tower, yang menambahkan lapisan otomatisasi AWS terkelola ke Organizations dan secara otomatis mengintegrasikannya dengan AWS layanan lain seperti AWS CloudTrail, AWS Config, Amazon CloudWatch, AWS Service Catalog, dan lainnya. Layanan ini dapat dikenakan biaya tambahan. Untuk informasi selengkapnya, lihat [harga AWS Control Tower](#).

Lihat juga

- [Kapan harus menggunakan AWS Organizations](#)
- [Kapan harus menggunakan AWS Control Tower](#)

Kapan harus menggunakan AWS Organizations

AWS Organizations adalah AWS layanan yang dapat Anda gunakan untuk mengelola Anda Akun AWS sebagai grup. Ini menyediakan fitur seperti penagihan konsolidasi, di mana semua tagihan akun Anda dikelompokkan bersama dan ditangani oleh satu pembayar. Anda juga dapat mengelola keamanan organisasi secara terpusat dengan menggunakan kontrol berbasis kebijakan. Untuk informasi selengkapnya AWS Organizations, lihat [Panduan AWS Organizations Pengguna](#).

Akses tepercaya

Ketika Anda menggunakan AWS Organizations untuk mengelola akun Anda sebagai grup, sebagian besar tugas administratif untuk organisasi hanya dapat dilakukan oleh akun manajemen organisasi. Secara default, ini hanya mencakup operasi yang terkait dengan pengelolaan organisasi itu sendiri. Anda dapat memperluas fungsionalitas tambahan ini ke AWS layanan lain dengan mengaktifkan akses tepercaya antara Organizations dan layanan tersebut. Akses tepercaya memberikan izin ke AWS layanan yang ditentukan untuk mengakses informasi tentang organisasi dan akun yang dikandungnya. Saat Anda mengaktifkan akses tepercaya untuk Manajemen Akun, layanan Manajemen Akun memberikan izin kepada Organisasi dan akun pengelolaannya untuk mengakses metadata, seperti informasi kontak utama atau alternatif, untuk semua akun anggota organisasi.

Untuk informasi selengkapnya, lihat [Aktifkan akses tepercaya untuk AWS Pengelolaan Akun](#).

Admin yang didelegasikan

Setelah mengaktifkan akses tepercaya, Anda juga dapat memilih untuk menetapkan salah satu akun anggota Anda sebagai akun admin yang didelegasikan untuk Manajemen AWS Akun. Hal ini memungkinkan akun admin yang didelegasikan untuk melakukan tugas pengelolaan metadata Manajemen Akun yang sama untuk akun anggota di organisasi Anda yang sebelumnya hanya dapat dilakukan oleh akun manajemen. Akun admin yang didelegasikan hanya dapat mengakses tugas manajemen untuk layanan Manajemen Akun. Akun admin yang didelegasikan tidak memiliki semua akses administratif ke organisasi yang dimiliki akun manajemen.

Untuk informasi selengkapnya, lihat [Mengaktifkan akun admin yang didelegasikan untuk Manajemen AWS Akun](#).

Kebijakan kontrol layanan

Ketika Anda Akun AWS adalah bagian dari organisasi yang dikelola oleh AWS Organizations, maka administrator organisasi dapat menerapkan [kebijakan kontrol layanan \(SCPs\)](#) yang dapat membatasi apa yang dapat dilakukan oleh prinsipal di akun anggota. SCP tidak pernah memberikan izin; sebaliknya, ini adalah filter yang membatasi izin apa yang dapat digunakan oleh akun anggota. Pengguna atau peran (prinsipal) dalam akun anggota hanya dapat melakukan operasi yang berada di persimpangan apa yang diizinkan oleh SCPs yang berlaku untuk akun dan kebijakan izin IAM yang dilampirkan pada kepala sekolah. Misalnya, Anda dapat menggunakan SCPs untuk mencegah prinsipal dalam akun memodifikasi kontak alternatif akun mereka sendiri.

Misalnya SCPs yang berlaku untuk Akun AWS, lihat [Batasi akses menggunakan kebijakan kontrol AWS Organizations layanan](#).

Aktifkan akses tepercaya untuk AWS Pengelolaan Akun

Mengaktifkan akses tepercaya untuk Manajemen AWS Akun memungkinkan administrator akun manajemen untuk mengubah informasi dan metadata (misalnya, detail kontak primer atau alternatif) khusus untuk setiap akun anggota. AWS Organizations Untuk informasi selengkapnya, lihat [Manajemen AWS Akun dan AWS Organizations](#) di Panduan AWS Organizations Pengguna. Untuk informasi umum tentang cara kerja akses tepercaya, lihat [Menggunakan AWS Organizations dengan AWS layanan lain](#).

Setelah akses tepercaya diaktifkan, Anda dapat menggunakan accountID parameter dalam [operasi API Manajemen Akun](#) yang mendukungnya. Anda dapat menggunakan parameter ini dengan sukses hanya jika Anda memanggil operasi menggunakan kredensi dari akun manajemen, atau dari akun admin yang didelegasikan untuk organisasi Anda jika Anda mengaktifkannya. Untuk informasi selengkapnya, lihat [Mengaktifkan akun admin yang didelegasikan untuk Manajemen AWS Akun](#).

Gunakan prosedur berikut untuk mengaktifkan akses tepercaya untuk Manajemen Akun di organisasi Anda.

Izin minimum

Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:

- Anda dapat melakukan ini hanya dari akun manajemen organisasi.
- Organisasi Anda harus [mengaktifkan semua fitur](#).

Konsol Manajemen AWS

Untuk mengaktifkan akses tepercaya untuk AWS Pengelolaan Akun

1. Masuklah ke [konsol AWS Organizations](#). Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak direkomendasikan) di akun pengelolaan organisasi.
2. Pilih Layanan di panel navigasi.
3. Pilih Manajemen AWS Akun dalam daftar layanan.
4. Pilih Aktifkan akses tepercaya.
5. Di kotak dialog Aktifkan akses tepercaya untuk Manajemen AWS Akun, ketik aktifkan untuk mengonfirmasinya, lalu pilih Aktifkan akses tepercaya.

AWS CLI & SDKs

Untuk mengaktifkan akses tepercaya untuk AWS Pengelolaan Akun

Setelah menjalankan perintah berikut, Anda dapat menggunakan kredensi dari akun manajemen organisasi untuk memanggil operasi API Manajemen Akun yang menggunakan `--accountId` parameter untuk mereferensikan akun anggota dalam organisasi.

- AWS CLI: [mengaktifkan akses layanan aws](#)

Contoh berikut memungkinkan akses tepercaya untuk Manajemen AWS Akun di organisasi akun panggilan.

```
$ aws organizations enable-aws-service-access \  
--service-principal account.amazonaws.com
```

Perintah ini tidak menghasilkan output jika berhasil.

Mengaktifkan akun admin yang didelegasikan untuk Manajemen AWS Akun

Anda mengaktifkan akun admin yang didelegasikan sehingga Anda dapat memanggil operasi API Manajemen AWS Akun untuk akun anggota lainnya. AWS Organizations Setelah Anda mendaftarkan akun admin yang didelegasikan untuk organisasi Anda, pengguna dan peran di akun tersebut dapat memanggil operasi AWS CLI dan AWS SDK di `account` namespace yang dapat berfungsi dalam mode Organizations dengan mendukung parameter opsional. `AccountId`

Untuk mendaftarkan akun anggota di organisasi Anda sebagai akun admin yang didelegasikan, gunakan prosedur berikut.

AWS CLI & SDKs

Untuk mendaftarkan akun admin yang didelegasikan untuk layanan Manajemen Akun

Anda dapat menggunakan perintah berikut untuk mengaktifkan admin yang didelegasikan untuk layanan Manajemen Akun.

Izin minimum

Untuk melakukan tugas-tugas ini, Anda harus memenuhi persyaratan berikut:

- Anda dapat melakukan ini hanya dari akun manajemen organisasi.
- Organisasi Anda harus [mengaktifkan semua fitur](#).
- Anda harus [mengaktifkan akses tepercaya untuk Manajemen Akun di organisasi Anda](#).

Anda harus menentukan prinsip layanan berikut:

```
account.amazonaws.com
```

- AWS CLI: [register-delegated-administrator](#)

Contoh berikut mendaftarkan akun anggota organisasi sebagai admin yang didelegasikan untuk layanan Manajemen Akun.

```
$ aws organizations register-delegated-administrator \  
  --account-id 123456789012 \  
  --service-principal account.amazonaws.com
```

Perintah ini tidak menghasilkan output jika berhasil.

Setelah menjalankan perintah ini, Anda dapat menggunakan kredensial dari akun 123456789012 untuk memanggil Manajemen Akun AWS CLI dan operasi SDK API yang menggunakan `--account-id` parameter untuk mereferensikan akun anggota di organisasi.

Konsol Manajemen AWS

Tugas ini tidak didukung di konsol manajemen manajemen AWS akun. Anda dapat melakukan tugas ini hanya dengan menggunakan AWS CLI atau operasi API dari salah satu AWS SDKs.

Batasi akses menggunakan kebijakan kontrol AWS Organizations layanan

Topik ini menyajikan contoh yang menunjukkan bagaimana Anda dapat menggunakan kebijakan kontrol layanan (SCPs) AWS Organizations untuk membatasi apa yang dapat dilakukan pengguna dan peran dalam akun di organisasi Anda. Untuk informasi selengkapnya tentang kebijakan kontrol layanan, lihat topik berikut di Panduan AWS Organizations Pengguna:

- [Menciptakan SCPs](#)
- [Melampirkan SCPs ke OUs dan akun](#)
- [Strategi untuk SCPs](#)
- [Sintaks kebijakan SCP](#)

Example Contoh 1: Mencegah akun memodifikasi kontak alternatif mereka sendiri

Contoh berikut menyangkal operasi `DeleteAlternateContact` API `PutAlternateContact` dan dipanggil oleh akun anggota mana pun dalam [mode akun mandiri](#). Ini mencegah setiap prinsipal di akun yang terpengaruh mengubah kontak alternatif mereka sendiri.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "arn:aws:account::*:account" ]
    }
  ]
}
```

```
}
```

Example Contoh 2: Mencegah akun anggota mengubah kontak alternatif untuk akun anggota lain di organisasi

Contoh berikut menggeneralisasi Resource elemen ke "*", yang berarti bahwa itu berlaku untuk [permintaan mode mandiri dan permintaan mode organisasi](#). Ini berarti bahwa bahkan akun admin yang didelegasikan untuk Manajemen Akun, jika SCP berlaku untuk itu, diblokir untuk mengubah kontak alternatif apa pun untuk akun apa pun di organisasi.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Deny",
      "Action": [
        "account:PutAlternateContact",
        "account>DeleteAlternateContact"
      ],
      "Resource": [ "*" ]
    }
  ]
}
```

Example Contoh 3: Mencegah akun anggota di OU memodifikasi kontak alternatifnya sendiri

Contoh SCP berikut mencakup kondisi yang membandingkan jalur organisasi akun dengan daftar dua. OUs Hal ini mengakibatkan pemblokiran prinsipal di akun apa pun di yang ditentukan OUs dari memodifikasi kontak alternatif mereka sendiri.

Kapan harus menggunakan AWS Control Tower

AWS Organizations adalah layanan dasar yang memungkinkan Anda mengelola dan mengamankan seluruh AWS lingkungan Anda secara terpusat. Komponen penting dari pendekatan AWS Organizations-sentris ini adalah. AWS Control Tower AWS Control Tower bertindak sebagai konsol

manajemen dalam Organizations, menyediakan cara yang efisien untuk mengatur dan mengatur AWS lingkungan multi-akun yang aman dengan menerapkan praktik terbaik preskriptif.

Pendekatan praktik terbaik keamanan yang disediakan oleh AWS Control Tower memperluas kemampuan inti. AWS Organizations AWS Control Tower menerapkan serangkaian pagar pembatas preventif dan detektif untuk membantu memastikan organisasi dan akun Anda tetap selaras dengan standar keamanan dan kepatuhan yang direkomendasikan.

Dengan membangun AWS Organizations struktur yang dirancang dengan baik AWS Control Tower, Anda dapat dengan cepat menerapkan lingkungan yang terukur, aman, dan sesuai. AWS Pendekatan terpusat untuk manajemen dan tata kelola cloud ini sangat penting bagi perusahaan yang ingin memanfaatkan kekuatan penuh AWS Cloud sambil mempertahankan standar keamanan dan kepatuhan tertinggi.

Untuk informasi selengkapnya, lihat [Apa itu AWS Control Tower?](#) dalam Panduan Pengguna AWS Control Tower .

Memahami mode operasi API

Operasi API yang bekerja dengan atribut Akun AWS selalu bekerja di salah satu dari dua mode operasi:

- Konteks mandiri — mode ini digunakan saat pengguna atau peran dalam akun mengakses atau mengubah atribut akun di akun yang sama. Mode konteks mandiri secara otomatis digunakan saat Anda tidak menyertakan `AccountId` parameter saat memanggil salah satu operasi Manajemen Akun AWS CLI atau AWS SDK.
- Konteks Organizations — mode ini digunakan ketika pengguna atau peran dalam satu akun dalam organisasi mengakses atau mengubah atribut akun di akun anggota yang berbeda di organisasi yang sama. Mode konteks organisasi secara otomatis digunakan saat Anda menyertakan `AccountId` parameter saat Anda memanggil salah satu operasi Manajemen Akun AWS CLI atau AWS SDK. Anda dapat memanggil operasi dalam mode ini hanya dari akun manajemen organisasi, atau akun admin yang didelegasikan untuk Manajemen Akun.

Operasi AWS SDK AWS CLI dan SDK dapat bekerja dalam konteks mandiri atau organisasi.

- Jika Anda tidak menyertakan `AccountId` parameter, maka operasi berjalan dalam konteks mandiri dan secara otomatis menerapkan permintaan ke akun yang Anda gunakan untuk membuat permintaan. Ini benar apakah akun tersebut adalah anggota organisasi atau tidak.

- Jika Anda menyertakan AccountId parameter, maka operasi berjalan dalam konteks organisasi, dan operasi bekerja pada akun Organizations yang ditentukan.
 - Jika akun yang memanggil operasi adalah akun manajemen atau akun admin yang didelegasikan untuk layanan Manajemen Akun, maka Anda dapat menentukan akun anggota organisasi itu dalam AccountId parameter untuk memperbarui akun yang ditentukan.
 - Satu-satunya akun dalam organisasi yang dapat memanggil salah satu operasi kontak alternatif dan menentukan nomor akunnya sendiri dalam AccountId parameter adalah akun yang ditentukan sebagai akun [admin yang didelegasikan](#) untuk layanan Manajemen Akun. Akun lain, termasuk akun manajemen, menerima AccessDenied pengecualian.
- Jika Anda menjalankan operasi dalam mode mandiri, maka Anda harus diizinkan untuk menjalankan operasi dengan kebijakan IAM yang menyertakan Resource elemen baik "*" untuk mengizinkan semua sumber daya, atau [ARN yang menggunakan sintaks untuk akun mandiri](#).
- Jika Anda menjalankan operasi dalam mode organisasi, maka Anda harus diizinkan untuk menjalankan operasi dengan kebijakan IAM yang menyertakan Resource elemen baik "*" untuk mengizinkan semua sumber daya, atau [ARN yang menggunakan sintaks untuk akun anggota dalam](#) organisasi.

Memberikan izin untuk memperbarui atribut akun

Seperti kebanyakan AWS operasi, Anda memberikan izin untuk menambah, memperbarui, atau menghapus atribut akun Akun AWS dengan menggunakan kebijakan [izin IAM](#). Saat Anda melampirkan kebijakan izin IAM ke prinsipal IAM (baik pengguna atau peran), Anda menentukan tindakan mana yang dapat dilakukan prinsipal pada sumber daya mana, dan dalam kondisi apa.

Berikut ini adalah beberapa pertimbangan khusus Manajemen Akun untuk membuat kebijakan izin.

Format Nama Sumber Daya Amazon untuk Akun AWS

- [Nama Sumber Daya Amazon \(ARN\)](#) untuk Akun AWS yang dapat Anda sertakan dalam resource elemen pernyataan kebijakan dibuat secara berbeda berdasarkan apakah akun yang ingin Anda referensikan adalah akun mandiri atau akun yang ada di organisasi. Lihat bagian sebelumnya di [Memahami mode operasi API](#).

- Akun ARN untuk akun mandiri:

```
arn:aws:account::{AccountId}:account
```

Anda harus menggunakan format ini saat menjalankan operasi atribut akun dalam mode mandiri dengan tidak menyertakan AccountID parameter.

- Akun ARN untuk akun anggota dalam suatu organisasi:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Anda harus menggunakan format ini saat menjalankan operasi atribut akun dalam mode organisasi dengan menyertakan AccountID parameter.

Kunci konteks untuk kebijakan IAM

Layanan Manajemen Akun juga menyediakan beberapa [kunci kondisi khusus layanan Manajemen Akun](#) yang memberikan kontrol halus atas izin yang Anda berikan.

akun: AccountResourceOrgPaths

Kunci konteks `account:AccountResourceOrgPaths` memungkinkan Anda menentukan jalur melalui hierarki organisasi Anda ke unit organisasi tertentu (OU). Hanya akun anggota yang terkandung oleh OU tersebut yang cocok dengan kondisi tersebut. Contoh cuplikan berikut membatasi kebijakan agar hanya berlaku pada akun yang berada di salah satu dari dua OU yang ditentukan.

Karena `account:AccountResourceOrgPaths` adalah jenis string multi-nilai, Anda harus menggunakan [ForAnyValue atau ForAllValues multi-nilai operator string](#). Juga, perhatikan bahwa awalan pada kunci kondisi adalah `account`, meskipun Anda mereferensikan jalur ke OU dalam suatu organisasi.

```
"Condition": {
  "ForAnyValue:StringLike": {
    "account:AccountResourceOrgPaths": [
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*",
      "o-aa111bb222/r-a1b2/ou-a1b2-f6g7h222/*"
    ]
  }
}
```

akun: AccountResourceOrgTags

Kunci konteks `account:AccountResourceOrgTags` memungkinkan Anda mereferensikan tag yang dapat dilampirkan ke akun di organisasi. Tag adalah pasangan key/value string yang dapat Anda gunakan untuk mengkategorikan dan memberi label sumber daya di akun Anda. Untuk informasi selengkapnya tentang penandaan, lihat [Editor Tag](#) di Panduan AWS Resource Groups Pengguna. Untuk informasi tentang penggunaan tag sebagai bagian dari strategi kontrol akses berbasis atribut, lihat [Untuk apa ABAC AWS](#) dalam Panduan Pengguna IAM. Contoh cuplikan berikut membatasi kebijakan agar hanya berlaku pada akun di organisasi yang memiliki tag dengan kunci `project` dan nilai salah satu atau `blue` `red`

Karena `account:AccountResourceOrgTags` adalah jenis string multi-nilai, Anda harus menggunakan [ForAnyValueatau ForAllValues multi-nilai operator string](#). Juga, perhatikan bahwa awalan pada kunci kondisi adalah `account`, meskipun Anda mereferensikan tag pada akun anggota organisasi.

```
"Condition": {
  "ForAnyValue:StringLike": {
    "account:AccountResourceOrgTags/project": [
      "blue",
      "red"
    ]
  }
}
```

Note

Anda dapat melampirkan tag hanya ke akun di organisasi. Anda tidak dapat melampirkan tag ke standalone Akun AWS.

Konfigurasi Akun AWS

Bagian ini mencakup topik yang menjelaskan cara mengelola Akun AWS.

Note

Jika Anda Akun AWS dibuat di India dengan menggunakan Amazon Web Services India Private Limited (AWS India), ada pertimbangan tambahan. Lihat informasi yang lebih lengkap di [Kelola akun di India](#).

Topik

- [Buat Akun AWS alias](#)
- [Aktifkan atau nonaktifkan Wilayah AWS di akun Anda](#)
- [Perbarui tagihan untuk Anda Akun AWS](#)
- [Perbarui alamat email pengguna root](#)
- [Perbarui kata sandi pengguna root](#)
- [Perbarui Akun AWS name](#)
- [Perbarui kontak alternatif untuk Anda Akun AWS](#)
- [Perbarui kontak utama untuk Anda Akun AWS](#)
- [Tampilan Akun AWS pengidentifikasi](#)

Buat Akun AWS alias

Jika Anda ingin URL untuk pengguna IAM Anda berisi nama perusahaan Anda (atau easy-to-remember pengenalan lain) alih-alih Akun AWS ID, Anda dapat membuat alias akun.

Untuk mempelajari cara membuat atau memperbarui alias akun, lihat [Menggunakan alias untuk Akun AWS ID Anda di Panduan](#) Pengguna IAM.

Aktifkan atau nonaktifkan Wilayah AWS di akun Anda

Awilayah AWS adalah lokasi fisik di dunia di mana AWS memiliki beberapa Availability Zone. Availability Zones terdiri dari satu atau lebih pusat AWS data diskrit, masing-masing dengan

daya redundant, jaringan, dan konektivitas, ditempatkan di fasilitas terpisah. Ini berarti bahwa masing-masing Wilayah AWS secara fisik terisolasi dan independen dari Daerah lain. Wilayah memberikan toleransi kesalahan, stabilitas, serta ketahanan, dan juga dapat mengurangi latensi. Menjalankan beban kerja Wilayah AWS lebih dekat ke pengguna akhir dapat meningkatkan kinerja dan menurunkan latensi. Untuk peta Wilayah yang tersedia dan yang akan datang, lihat [Wilayah dan Zona Ketersediaan](#). [Untuk mempelajari lebih lanjut tentang Wilayah AWS dan arsitektur ketahanan untuk beban kerja Anda, kunjungi AWS Dasar-dasar multi-wilayah](#).

Wilayah AWS secara luas jatuh ke dalam dua kategori ketersediaan untuk akun:

- Wilayah Default - Wilayah yang diluncurkan sebelum 20 Maret 2019 diaktifkan secara default. Anda dapat membuat dan mengelola sumber daya di Wilayah default ini segera setelah aktivasi akun Anda. Wilayah Default tidak dapat diaktifkan atau dinonaktifkan.
- Opt-in Wilayah - Wilayah yang diluncurkan setelah 20 Maret 2019 dinonaktifkan secara default dan disebut sebagai Wilayah keikutsertaan. Wilayah keikutsertaan yang dinonaktifkan tidak ditampilkan di bilah Navigasi Konsol, dan Anda tidak dapat menggunakan Wilayah ini untuk membuat beban kerja hingga diaktifkan. Untuk menggunakan Wilayah keikutsertaan ini, Anda harus terlebih dahulu mengaktifkannya di wilayah Anda Akun AWS. Setelah mengaktifkan Wilayah keikutsertaan, Anda dapat memilih Wilayah tersebut di bilah navigasi dan membuat serta mengelola sumber daya di Wilayah tersebut. Untuk mengaktifkan Wilayah keikutsertaan untuk akun mandiri Anda, lihat [Mengaktifkan atau menonaktifkan Region untuk akun mandiri](#) dan aktifkan Wilayah keikutsertaan untuk akun anggota Anda, lihat [Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda](#)

Saat Anda mendaftar Akun AWS, AWS merekomendasikan Wilayah keikutsertaan untuk Anda berdasarkan negara alamat kontak Anda. Pelanggan di negara dengan Wilayah AWS keikutsertaan melihat rekomendasi di halaman Informasi Kontak untuk mengaktifkan Wilayah keikutsertaan di negara tersebut. Pelanggan di negara dengan Wilayah keikutsertaan dan Wilayah default, seperti India, Australia, atau Kanada, melihat rekomendasi untuk memilih Wilayah keikutsertaan jika Wilayah keikutsertaan lebih dekat dengan mereka daripada Wilayah default. Setelah akun diaktifkan, Anda dapat mengaktifkan Wilayah AWS keikutsertaan lainnya di akun Anda atau memilih untuk menonaktifkan Wilayah keikutsertaan yang Anda aktifkan saat mendaftar.

Saat Anda membuat Akun AWS, data dan kredensial IAM Anda secara otomatis dikonfigurasi untuk bekerja di semua Wilayah default, memungkinkan pengguna root dan identitas IAM dengan izin yang sesuai untuk mengakses AWS layanan di Wilayah ini menggunakan kredensialnya yang ada. AWS Wilayah keikutsertaan dinonaktifkan secara default, dan data serta kredensialnya IAM pada awalnya tidak tersedia di Wilayah ini, yang mencegah akses ke AWS layanan di Wilayah tersebut. Saat Anda

memilih untuk mengaktifkan Wilayah keikutsertaan, AWS menyebarkan data dan kredensi IAM Anda ke Wilayah tersebut. Setelah propagasi selesai dan Wilayah keikutsertaan diaktifkan, pengguna root dan identitas IAM kemudian dapat mengakses AWS layanan di Wilayah keikutsertaan yang baru diaktifkan menggunakan kredensial IAM yang sama yang mereka gunakan di Wilayah default.

Saat Anda menonaktifkan Wilayah keikutsertaan, kredensial IAM Anda dinonaktifkan dan Anda kehilangan akses IAM ke sumber daya di Wilayah keikutsertaan tersebut. Menonaktifkan Wilayah keikutsertaan tidak menghapus sumber daya di Wilayah tersebut dan biaya untuk sumber daya (jika ada) di Wilayah keikutsertaan yang dinonaktifkan tersebut terus bertambah dengan tarif standar.

Important

Menonaktifkan Wilayah menonaktifkan akses IAM ke sumber daya di Wilayah. Ini tidak menghapus sumber daya yang dimaksud, yang terus dikenakan biaya. Hapus sumber daya yang tersisa sebelum menonaktifkan Wilayah.

AWS mengelompokkan Wilayah menjadi [partisi](#). Setiap Wilayah berada dalam satu partisi, dan setiap partisi memiliki satu atau lebih Wilayah. Partisi memiliki instance independen AWS Identity and Access Management (IAM) dan memberikan batas keras antara Wilayah di partisi yang berbeda. AWS Daerah komersial berada di `aws` partisi, Wilayah di Tiongkok berada di `aws-cn` partisi, AWS GovCloud (US) dan Wilayah berada di `aws-us-gov` partisi. Tergantung pada partisi tempat Anda membuat Akun AWS, Anda dapat menggunakan Wilayah AWS di dalam partisi itu.

- Akun di `aws` partisi memberi Anda akses ke beberapa Wilayah di partisi komersial sehingga Anda dapat meluncurkan AWS sumber daya di lokasi yang memenuhi kebutuhan Anda. Misalnya, Anda mungkin ingin meluncurkan instans Amazon EC2 di Eropa agar lebih dekat dengan pelanggan Eropa Anda atau untuk memenuhi persyaratan hukum.
- Akun di `aws-us-gov` partisi memberi Anda akses ke Wilayah AWS GovCloud (US-West) dan Wilayah AWS GovCloud (US-East). Untuk informasi selengkapnya, lihat [AWS GovCloud \(US\)](#).
- Akun di `aws-cn` partisi memberi Anda akses ke Wilayah Beijing dan Ningxia saja. Untuk informasi selengkapnya, lihat [Amazon Web Services di Tiongkok](#).

Topik

- [Referensi ketersediaan regional](#)
- [Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah](#)

- [Waktu pemrosesan dan batas permintaan](#)
- [Mengaktifkan atau menonaktifkan Region untuk akun mandiri](#)
- [Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda](#)

Referensi ketersediaan regional

Daftar tabel berikut Wilayah AWS berdasarkan jenis ketersediaan. Wilayah Default diaktifkan secara otomatis dan tidak dapat dinonaktifkan, sementara Wilayah keikutsertaan harus diaktifkan secara manual sebelum Anda dapat menggunakannya:

Opt-in Regions

Wilayah berikut adalah Wilayah keikutsertaan yang harus diaktifkan sebelum Anda dapat menggunakannya:

Nama	Kode	Status
Africa (Cape Town)	af-south-1	GA
Asia Pasifik (Hong Kong)	ap-east-1	GA
Asia Pasifik (Taipei)	ap-east-2	GA
Asia Pasifik (Hyderabad)	ap-south-2	GA
Asia Pasifik (Jakarta)	ap-southeast-3	GA
Asia Pacific (Melbourne)	ap-southeast-4	GA
Asia Pasifik (Malaysia)	ap-southeast-5	GA
Asia Pasifik (Selandia Baru)	ap-southeast-6	GA
Asia Pasifik (Thailand)	ap-southeast-7	GA
Kanada Barat (Calgary)	ca-west-1	GA
Europe (Zurich)	eu-central-2	GA
Europe (Milan)	eu-south-1	GA

Nama	Kode	Status
Eropa (Spanyol)	eu-south-2	GA
Israel (Tel Aviv)	il-central-1	GA
Timur Tengah (UAE)	me-central-1	GA
Timur Tengah (Bahrain)	me-south-1	GA
Meksiko (Tengah)	mx-central-1	GA

Default Regions

Wilayah berikut diaktifkan secara default dan tidak dapat dinonaktifkan:

Nama	Kode
Asia Pasifik (Tokyo)	ap-northeast-1
Asia Pasifik (Seoul)	ap-northeast-2
Asia Pasifik (Osaka)	ap-northeast-3
Asia Pasifik (Mumbai)	ap-south-1
Asia Pasifik (Singapura)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Kanada (Pusat)	ca-central-1
Eropa (Frankfurt)	eu-central-1
Eropa (Stockholm)	eu-north-1
Eropa (Irlandia)	eu-west-1
Eropa (London)	eu-west-2

Nama	Kode
Eropa (Paris)	eu-west-3
Amerika Selatan (São Paulo)	sa-east-1
AS Timur (Virginia Utara)	us-east-1
AS Timur (Ohio)	us-east-2
AS Barat (California Utara)	us-west-1
AS Barat (Oregon)	us-west-2

Untuk daftar nama Wilayah dan kode yang sesuai, lihat [Titik akhir Regional](#) di Panduan Referensi AWS Umum. Untuk daftar AWS layanan yang didukung di setiap Wilayah (tanpa titik akhir), lihat [Daftar Layanan AWS Regional](#).

Important

AWS merekomendasikan agar Anda menggunakan titik akhir regional AWS Security Token Service (AWS STS) alih-alih titik akhir global untuk mengurangi latensi. Token sesi dari AWS STS titik akhir regional berlaku di semua AWS Wilayah. Jika Anda menggunakan AWS STS titik akhir regional, Anda tidak perlu melakukan perubahan apa pun. Namun, token sesi dari AWS STS titik akhir global (<https://sts.amazonaws.com>) hanya valid jika Anda mengaktifkan, atau yang diaktifkan secara default. Wilayah AWS Jika Anda bermaksud mengaktifkan Wilayah baru untuk akun Anda, Anda dapat menggunakan token sesi dari AWS STS titik akhir regional atau mengaktifkan AWS STS titik akhir global untuk mengeluarkan token sesi yang valid di semua Wilayah AWS. Token sesi yang valid di semua Wilayah memiliki ukuran yang lebih besar. Jika Anda menyimpan token sesi, token yang lebih besar ini dapat memengaruhi sistem Anda. Untuk informasi selengkapnya tentang cara kerja AWS STS titik akhir dengan AWS Wilayah, lihat [Mengelola AWS STS di AWS Wilayah](#).

Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah

Sebelum Anda mengaktifkan atau menonaktifkan Region, penting untuk mempertimbangkan hal berikut:

- Anda dapat menggunakan semua Wilayah tujuan dalam geografi inferensi lintas wilayah apa pun Region-opt statusnya — Layanan AI AWS generatif tertentu termasuk Amazon Bedrock (lihat [Meningkatkan throughput dengan inferensi Lintas wilayah](#)) dan [Pengembang Amazon Q](#) (lihat [pemrosesan Cross-region di Pengembang Amazon Q](#)) menggunakan inferensi lintas wilayah. Jika Anda menggunakan layanan tersebut, mereka secara otomatis memilih yang optimal Wilayah AWS- termasuk Wilayah yang belum Anda aktifkan untuk sumber daya dan data IAM - dalam geografi pilihan Anda. Ini meningkatkan pengalaman pelanggan dengan memaksimalkan ketersediaan komputasi dan model yang tersedia.
- Anda dapat menggunakan izin IAM untuk mengontrol akses ke Wilayah — AWS Identity and Access Management (IAM) mencakup empat izin yang memungkinkan Anda mengontrol pengguna mana yang dapat mengaktifkan, menonaktifkan, mendapatkan, dan mencantumkan Wilayah. Untuk informasi selengkapnya, lihat [AWS: Mengizinkan mengaktifkan dan menonaktifkan Wilayah AWS di Panduan Pengguna IAM](#). Anda juga dapat menggunakan tombol `aws:RequestedRegion` kondisi untuk mengontrol akses ke Layanan AWS dalam file Wilayah AWS.
- Mengaktifkan dan menonaktifkan Wilayah gratis - Tidak ada biaya untuk mengaktifkan atau menonaktifkan Wilayah. Anda hanya dikenakan biaya untuk sumber daya yang Anda buat di Wilayah baru.
- EventBridge Integrasi Amazon - Anda dapat berlangganan pemberitahuan pembaruan status pilihan wilayah di EventBridge EventBridgePemberitahuan akan dibuat untuk setiap perubahan status, memungkinkan pelanggan untuk mengotomatiskan alur kerja.
- Region-opt Status ekspresif — Karena sifat asinkron dari wilayah enabling/disabling opt-in, ada empat status potensial untuk permintaan region-opt:
 - ENABLING
 - DISABLING
 - ENABLED
 - DISABLED

Anda tidak dapat membatalkan opt-in atau opt-out ketika berada dalam salah satu atau ENABLING status. DISABLING Kalau tidak, `ConflictException` akan dilemparkan. Permintaan region-opt yang diselesaikan (Enabled/Disabled) bergantung pada penyediaan layanan utama yang mendasari. AWS Mungkin ada beberapa AWS layanan yang tidak akan segera dapat digunakan meskipun statusnya ENABLED.

Waktu pemrosesan dan batas permintaan

Saat mengaktifkan atau menonaktifkan Wilayah, perhatikan batasan waktu dan permintaan berikut:

- Mengaktifkan Wilayah membutuhkan waktu beberapa menit hingga beberapa jam dalam beberapa kasus — Saat Anda mengaktifkan Wilayah, AWS lakukan tindakan untuk menyiapkan akun Anda di Wilayah tersebut, seperti mendistribusikan sumber daya IAM Anda ke Wilayah tersebut. Proses ini memakan waktu beberapa menit untuk sebagian besar akun, tetapi terkadang bisa memakan waktu beberapa jam. Anda tidak dapat menggunakan Wilayah sampai proses ini selesai.
- Menonaktifkan Wilayah tidak selalu langsung terlihat — Layanan dan konsol mungkin terlihat sementara setelah menonaktifkan suatu wilayah. Menonaktifkan suatu Wilayah dapat memakan waktu beberapa menit hingga beberapa jam untuk diterapkan.
- Satu akun dapat memiliki 6 permintaan pilihan wilayah yang sedang berlangsung pada waktu tertentu - Satu permintaan sama dengan mengaktifkan atau menonaktifkan satu wilayah tertentu untuk satu akun.
- Organizations dapat memiliki 50 permintaan region-opt terbuka pada waktu tertentu di seluruh AWS organisasi — Akun manajemen dapat kapan saja memiliki 50 permintaan terbuka yang menunggu penyelesaian untuk organisasinya. Satu permintaan sama dengan mengaktifkan atau menonaktifkan satu wilayah tertentu untuk satu akun.

Mengaktifkan atau menonaktifkan Region untuk akun mandiri

Untuk memperbarui Wilayah mana yang dapat Anda Akun AWS akses, lakukan langkah-langkah dalam prosedur berikut. Konsol Manajemen AWS Prosedur di bawah ini selalu berfungsi hanya dalam konteks mandiri. Anda dapat menggunakan Konsol Manajemen AWS untuk melihat atau memperbarui hanya Wilayah yang tersedia di akun yang Anda gunakan untuk memanggil operasi.

Konsol Manajemen AWS

Untuk mengaktifkan atau menonaktifkan Region untuk standalone Akun AWS

Izin minimum

Untuk melakukan langkah-langkah dalam prosedur berikut, pengguna atau peran IAM harus memiliki izin berikut:

- `account:ListRegions`(diperlukan untuk melihat daftar Wilayah AWS dan apakah mereka saat ini diaktifkan atau dinonaktifkan).

- `account:EnableRegion`
- `account:DisableRegion`

1. Masuk ke [Konsol Manajemen AWS](#) sebagai Pengguna root akun AWS atau sebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Pada [halaman Akun](#), gulir ke bawah ke bagian Wilayah AWS.
4. Pilih Wilayah yang ingin Anda aktifkan atau nonaktifkan dan kemudian pilih tindakan yang diinginkan Aktifkan atau Nonaktifkan. Anda akan melihat prompt untuk mengonfirmasi.
5. Jika Anda memilih opsi Aktifkan, tinjau teks yang ditampilkan dan kemudian pilih Aktifkan wilayah.

Jika Anda memilih opsi Nonaktifkan, tinjau teks yang ditampilkan, ketik **disable** untuk mengonfirmasi, lalu pilih Nonaktifkan wilayah.

Setelah Region opt-in diaktifkan, Anda dapat memilih Region tersebut dari bilah navigasi Region. Untuk langkah-langkah memilih Wilayah, lihat [Memilih Wilayah dari bilah navigasi di Konsol Manajemen AWS](#) dan untuk pengaturan konsol khusus Wilayah di akun Anda, lihat [Menyetel Wilayah default di Konsol Manajemen AWS](#).

AWS CLI & SDKs

Anda dapat mengaktifkan, menonaktifkan, membaca, dan mencantumkan status pilihan wilayah dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki izin yang memetakan ke operasi itu:

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account:ListRegions`

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi pilihan wilayah, dan memberi orang lain kemampuan untuk membaca dan menulis.

Contoh berikut memungkinkan wilayah untuk akun anggota tertentu dalam organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

Perhatikan bahwa Anda juga dapat menonaktifkan wilayah menggunakan perintah yang sama dan kemudian menggantinya `enable-region` dengan `disable-region`.

```
aws account enable-region --region-name af-south-1
```

Perintah ini tidak menghasilkan output jika berhasil.

Operasi ini asinkron. Perintah berikut akan memungkinkan Anda untuk melihat status permintaan terbaru.

```
aws account get-region-opt-status --region-name af-south-1
{
  "RegionName": "af-south-1",
  "RegionOptStatus": "ENABLING"
}
```

Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

Untuk memperbarui Wilayah yang diaktifkan untuk akun anggota Anda AWS Organizations, lakukan langkah-langkah dalam prosedur berikut.

Note

Kebijakan AWS Organizations terkelola `AWSOrganizationsReadOnlyAccess` atau `AWSOrganizationsFullAccess` diperbarui untuk memberikan izin mengakses API Manajemen AWS Akun sehingga Anda dapat mengakses data akun dari AWS Organizations konsol. Untuk melihat kebijakan terkelola yang diperbarui, lihat Kebijakan yang [AWS dikelola Update to Organizations](#).

Note

Sebelum Anda dapat melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi untuk digunakan dengan akun anggota, Anda harus:

- Aktifkan semua fitur di organisasi Anda untuk mengelola pengaturan di akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat [Mengaktifkan semua fitur di](#) organisasi Anda.
- Aktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihat [Aktifkan akses tepercaya untuk AWS Pengelolaan Akun](#).

Konsol Manajemen AWS

Untuk mengaktifkan atau menonaktifkan Wilayah di organisasi Anda

1. Masuk ke AWS Organizations konsol dengan kredensial akun manajemen organisasi Anda.
2. Pada Akun AWS Halaman, pilih akun yang ingin Anda perbarui.
3. Pilih tab Pengaturan akun.
4. Di bawah Wilayah, pilih Wilayah yang ingin Anda aktifkan atau nonaktifkan.
5. Pilih Tindakan, lalu pilih opsi Aktifkan atau Nonaktifkan.
6. Jika Anda memilih opsi Aktifkan, tinjau teks yang ditampilkan dan kemudian pilih Aktifkan wilayah.
7. Jika Anda memilih opsi Nonaktifkan, tinjau teks yang ditampilkan, ketik nonaktifkan untuk mengonfirmasi, lalu pilih Nonaktifkan wilayah.

AWS CLI & SDKs

Anda dapat mengaktifkan, menonaktifkan, membaca, dan mencantumkan status pilihan wilayah untuk akun anggota organisasi dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- `EnableRegion`
- `DisableRegion`
- `GetRegionOptStatus`
- `ListRegions`

Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki izin yang memetakan ke operasi itu:

- `account:EnableRegion`
- `account:DisableRegion`
- `account:GetRegionOptStatus`
- `account>ListRegions`

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca informasi pilihan wilayah, dan memberi orang lain kemampuan untuk membaca dan menulis.

Contoh berikut memungkinkan wilayah untuk akun anggota tertentu dalam organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

Perhatikan bahwa Anda juga dapat menonaktifkan wilayah menggunakan perintah yang sama dan kemudian menggantinya `enable-region` dengan `disable-region`.

```
aws account enable-region --account-id 123456789012 --region-name af-south-1
```

Perintah ini tidak menghasilkan output jika berhasil.

Note

Sebuah organisasi hanya dapat memiliki hingga 20 permintaan wilayah pada waktu tertentu. Jika tidak, Anda akan menerima `aTooManyRequestsException`.

Operasi ini asinkron. Perintah berikut akan memungkinkan Anda untuk melihat status permintaan terbaru.

```
aws account get-region-opt-status --account-id 123456789012 --region-name af-south-1
{
  "RegionName": "af-south-1",
  "RegionOptStatus": "ENABLING"
}
```

Perbarui tagihan untuk Anda Akun AWS

Anda dapat memperbarui semua preferensi Akun AWS penagihan menggunakan konsol AWS Billing dan Manajemen Biaya. [Untuk mempelajari cara memperbarui setelan terkait penagihan untuk akun Anda, lihat Panduan Pengguna:AWS Manajemen Penagihan dan Biaya](#)

Perbarui alamat email pengguna root

Ada berbagai alasan bisnis mengapa Anda mungkin perlu memperbarui alamat email pengguna root Anda Akun AWS. Misalnya, keamanan dan ketahanan administratif. Topik ini memandu Anda melalui proses memperbarui alamat email pengguna root Anda alamat email untuk akun mandiri dan akun anggota.

Note

Perubahan pada an Akun AWS bisa memakan waktu hingga empat jam untuk menyebar ke mana-mana.

Anda dapat memperbarui email pengguna root email secara berbeda, tergantung pada apakah akun berdiri sendiri atau tidak, atau bagian dari organisasi:

- Mandiri Akun AWS — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui email pengguna root menggunakan AWS Management Console. Untuk mempelajari cara melakukannya, lihat [Memperbarui email pengguna root email untuk mandiri Akun AWS](#).
- Akun AWS dalam organisasi — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui email pengguna root email dari akun anggota dari AWS Organizations konsol, atau secara terprogram melalui CLI AWS & SDK. Untuk mempelajari cara melakukannya, lihat [Memperbarui email pengguna root untuk semua orang Akun AWS di organisasi Anda](#).

Topik

- [Perbarui email pengguna root untuk standalone Akun AWS atau akun manajemen](#)
- [Perbarui email pengguna root untuk setiap Akun AWS di organisasi Anda](#)

Perbarui email pengguna root untuk standalone Akun AWS atau akun manajemen

Untuk mengedit alamat email pengguna root alamat untuk mandiri Akun AWS, lakukan langkah-langkah dalam prosedur berikut.


Konsol Manajemen AWS

Note

Anda harus masuk sebagai Pengguna root akun AWS, yang tidak memerlukan izin IAM tambahan. Anda tidak dapat melakukan langkah-langkah ini sebagai pengguna atau peran IAM.

1. Gunakan alamat email dan kata sandi Anda untuk masuk ke [Konsol Manajemen AWS](#) sebagai Akun AWS milik Anda Pengguna root akun AWS.
2. Di sudut kanan atas konsol, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada [halaman Akun](#), di samping Detail akun, pilih Tindakan, lalu pilih Perbarui alamat email dan kata sandi.
4. Pada halaman Detail Akun, di samping Alamat email pilih Edit.

5. Pada halaman Edit Email Akun, isi kolom untuk Alamat email baru, Konfirmasikan alamat email baru, dan konfirmasikan Kata Sandi Anda saat ini. Kemudian, pilih Simpan dan lanjutkan. Kode verifikasi dikirim ke alamat email baru Anda darino-reply@verify.signin.aws.
6. Pada halaman Edit Email Akun, di bawah kode Verifikasi, masukkan kode yang Anda terima dari email Anda, lalu pilih Konfirmasi pembaruan.

 Note


Diperlukan waktu hingga 5 menit agar kode verifikasi tiba. Jika Anda tidak melihat email di kotak masuk, periksa folder spam dan sampah Anda.

AWS CLI & SDKs

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

Perbarui email pengguna root untuk setiap Akun AWS di organisasi Anda

Untuk mengedit alamat email pengguna root alamat untuk setiap akun anggota di organisasi Anda menggunakan AWS Organizations konsol, lakukan langkah-langkah dalam prosedur berikut.

 Note

Sebelum Anda memperbarui alamat email pengguna root alamat untuk akun anggota, kami sarankan Anda memahami dampak dari operasi ini. Untuk informasi selengkapnya, lihat [Memperbarui alamat email pengguna root untuk akun anggota AWS Organizations](#) di Panduan AWS Organizations Pengguna.

Anda juga dapat memperbarui alamat email pengguna root alamat untuk akun anggota langsung dari [halaman Akun](#) Konsol Manajemen AWS setelah masuk sebagai pengguna root. Untuk petunjuk langkah demi langkah, ikuti langkah-langkah yang disediakan di [Perbarui email pengguna root untuk standalone Akun AWS atau akun manajemen](#).

AWS Management Console

Catatan

- Untuk melakukan prosedur ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus [mengaktifkan akses tepercaya untuk layanan Manajemen Akun](#).
- Anda tidak dapat menggunakan prosedur ini untuk mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

Untuk memperbarui alamat email pengguna root untuk akun anggota menggunakan AWS Organizations konsol

1. Masuk ke [konsol AWS Organizations](#) tersebut. Anda harus masuk sebagai pengguna IAM, atau masuk sebagai pengguna root ([tidak disarankan](#)) di akun manajemen organisasi.
2. Pada Akun AWSHalaman, pilih akun anggota yang ingin Anda perbarui alamat email pengguna root alamat email .
3. Di bagian Detail akun, pilih tombol Tindakan, lalu pilih Perbarui alamat email.
4. Di bawah Email, masukkan alamat email baru untuk pengguna root, lalu pilih Simpan. Ini mengirimkan kata sandi satu kali (OTP) ke alamat email baru.

Note

Jika Anda perlu menutup halaman ini di konsol Organizations sambil menunggu kode, Anda dapat mengembalikan dan menyelesaikan proses OTP dalam waktu 24 jam sejak kode dikirim. Untuk melakukannya, saat berada di halaman Detail akun, pilih tombol Tindakan, lalu pilih Selesaikan pembaruan email.

5. Di bawah Kode verifikasi, masukkan kode yang dikirim ke alamat email baru pada langkah sebelumnya, lalu pilih Konfirmasi. Ini melakukan pembaruan ke pengguna root untuk akun tersebut.

AWS CLI & SDKs

Anda dapat mengambil, atau memperbarui alamat email pengguna root (juga disebut sebagai alamat email utama) dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- [GetPrimaryEmail](#)
- [StartPrimaryEmailUpdate](#)
- [AcceptPrimaryEmailUpdate](#)

Catatan

- Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus [mengaktifkan akses tepercaya untuk layanan Manajemen Akun](#).
- Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

Izin minimum

Untuk setiap operasi, Anda harus memiliki izin yang memetakan operasi itu:

- `account:GetPrimaryEmail`
- `account:StartPrimaryEmailUpdate`
- `account:AcceptPrimaryEmailUpdate`

Jika Anda menggunakan izin individual ini, Anda dapat memberi beberapa pengguna kemampuan untuk hanya membaca alamat email pengguna root informasi alamat email , dan memberi orang lain kemampuan untuk membaca dan menulis.

Untuk menyelesaikan proses alamat email pengguna root , Anda harus menggunakan API email utama bersama-sama dalam urutan yang ditunjukkan pada contoh di bawah ini.

Example **GetPrimaryEmail**

Contoh berikut mengambil alamat email pengguna root alamat email dari akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account get-primary-email --account-id 123456789012
```

Example **StartPrimaryEmailUpdate**

Contoh berikut memulai proses pembaruan alamat email pengguna root baru, dan mengirimkan kata sandi satu kali (OTP) ke alamat email baru untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account start-primary-email-update --account-id 123456789012 --primary-email john@examplecorp.com
```

Example **AcceptPrimaryEmailUpdate**

Contoh berikut menerima kode OTP dan menetapkan alamat email baru ke akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account accept-primary-email-update --account-id 123456789012 --otp 12345678 --primary-email john@examplecorp.com
```

Perbarui kata sandi pengguna root

Untuk mengedit kata sandi pengguna root Anda Akun AWS, lakukan langkah-langkah dalam prosedur berikut.

Konsol Manajemen AWS

Untuk mengedit kata sandi pengguna root Anda

Note

Anda harus masuk sebagai Pengguna root akun AWS, yang tidak memerlukan izin IAM tambahan. Anda tidak dapat melakukan langkah-langkah ini sebagai pengguna atau peran IAM.

1. Gunakan alamat email dan kata sandi Anda untuk masuk ke [Konsol Manajemen AWS](#) sebagai Akun AWS milik Anda Pengguna root akun AWS.
2. Di sudut kanan atas konsol, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada [halaman Akun](#), di samping Detail akun, pilih Tindakan, lalu pilih Perbarui alamat email dan kata sandi.
4. Pada halaman Detail Akun, di samping Kata Sandi pilih Edit.
5. Pada halaman Edit kata sandi, isi kolom untuk Kata sandi saat ini, Kata sandi baru, dan Konfirmasi kata sandi baru. Kemudian, pilih Perbarui kata sandi. Untuk panduan tambahan termasuk praktik terbaik untuk menyetel kata sandi pengguna root, lihat [Mengubah kata sandi untuk](#) Panduan Pengguna IAM. Pengguna root akun AWS

AWS CLI & SDKs

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDKs. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

Perbarui Akun AWS name

Saat mengelola beberapa Akun AWS, gunakan konvensi penamaan yang jelas yang selaras dengan unit bisnis dan aplikasi untuk identifikasi dan organisasi. Selama reorganisasi, merger, akuisisi, atau pembaruan konvensi penamaan, Anda mungkin perlu mengganti nama akun untuk mempertahankan identifikasi dan standar administrasi yang konsisten.

Nama akun muncul di beberapa tempat, seperti di faktur Anda dan di konsol seperti dasbor Billing and Cost Management dan konsol. AWS Organizations Kami menyarankan Anda menggunakan

cara standar untuk memberi nama akun Anda sehingga nama akun Anda mudah dikenali. Untuk akun perusahaan, pertimbangkan untuk menggunakan standar penamaan seperti organisasi - tujuan - lingkungan (misalnya, penjualan - katalog - prod). Untuk alasan privasi dan keamanan, hindari menggunakan nama akun yang mencerminkan informasi identitas pribadi (PII).

- **Mandiri Akun AWS** — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui nama akun menggunakan Konsol Manajemen AWS, atau SDK AWS CLI dan. Untuk mempelajari cara melakukannya, lihat [Perbarui nama akun Anda untuk standalone Akun AWS](#).
- **Akun AWS dalam organisasi** — Untuk akun anggota yang merupakan bagian dari sebuah AWS Organizations, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui nama akun akun anggota mana pun di organisasi secara terpusat dari AWS Organizations konsol, atau secara terprogram melalui dan SDK. AWS CLI Untuk mempelajari cara melakukannya, lihat [Perbarui nama akun Anda untuk apa pun Akun AWS di organisasi Anda](#).

Note

Perubahan pada an Akun AWS bisa memakan waktu hingga empat jam untuk menyebar ke mana-mana.

Topik

- [Perbarui nama akun Anda untuk standalone Akun AWS](#)
- [Perbarui nama akun Anda untuk apa pun Akun AWS di organisasi Anda](#)

Perbarui nama akun Anda untuk standalone Akun AWS

Untuk mengubah nama akun untuk mandiri Akun AWS, lakukan langkah-langkah dalam prosedur berikut.

Konsol Manajemen AWS

Izin minimum

Anda dapat memperbarui nama akun Anda menggunakan pengguna root, pengguna IAM, atau peran IAM. Jika Anda menggunakan pengguna root, tidak ada izin IAM tambahan yang diperlukan untuk memperbarui nama akun. Saat menggunakan pengguna IAM atau peran IAM, Anda harus memiliki setidaknya izin IAM berikut:

- `account:GetAccountInformation`
- `account:PutAccountName`

Untuk memperbarui nama akun untuk akun mandiri

1. Gunakan alamat email dan kata sandi Anda untuk masuk ke [Konsol Manajemen AWS](#) sebagai Akun AWS milik Anda Pengguna root akun AWS.
2. Di sudut kanan atas konsol, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada [halaman Akun](#), di samping Detail akun, pilih Tindakan, lalu pilih Perbarui nama akun.
4. Di bawah Nama, masukkan nama akun baru yang ingin Anda perbarui, lalu pilih Simpan.

AWS CLI & SDKs

Izin minimum

Anda dapat memperbarui nama akun Anda menggunakan pengguna root, pengguna IAM, atau peran IAM. Untuk melakukan langkah-langkah berikut, pengguna IAM atau peran IAM Anda harus memiliki setidaknya izin IAM berikut:

- `account:GetAccountInformation`
- `account:PutAccountName`

Untuk memperbarui nama akun untuk akun mandiri

Anda dapat menggunakan salah satu operasi berikut:

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
    --account-name "New-Account-Name"
```

- AWS SDK: [PutAccountName](#)

Perbarui nama akun Anda untuk apa pun Akun AWS di organisasi Anda

AWS Organizations Dengan mode semua fitur, pengguna IAM resmi atau peran IAM di akun admin manajemen dan yang didelegasikan dapat mengelola nama akun secara terpusat.

Untuk mengubah nama akun untuk setiap akun anggota di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan

Untuk memperbarui nama akun dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat [Mengaktifkan semua fitur untuk organisasi](#).
- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihat [Aktifkan akses tepercaya untuk AWS Pengelolaan Akun](#).

Konsol Manajemen AWS

Izin minimum

Untuk memperbarui nama akun akun anggota, pengguna IAM atau peran IAM Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` (hanya konsol)
- `account:PutAccountName`

Untuk memperbarui nama akun untuk akun anggota

1. Buka konsol Organizations di <https://console.aws.amazon.com/organizations/>.
2. Di panel navigasi kiri, pilih Akun AWS.
3. Pada Akun AWS, pilih akun anggota yang ingin Anda perbarui, pilih menu tarik-turun Tindakan, lalu pilih Perbarui nama akun.
4. Di bawah Nama, masukkan nama yang diperbarui, dan pilih Simpan.

AWS CLI & SDKs

Izin minimum

Untuk memperbarui nama akun akun anggota, pengguna IAM atau peran IAM Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` (hanya konsol)
- `account:PutAccountName`

Untuk memperbarui nama akun untuk akun anggota

Anda dapat menggunakan salah satu operasi berikut:

- AWS CLI: [put-account-name](#)

```
$ C:\> aws account put-account-name \  
    --account-id 111111111111 \  
    --account-name "New-Account-Name"
```

- AWS SDK: [PutAccountName](#)

Perbarui kontak alternatif untuk Anda Akun AWS

Kontak alternatif memungkinkan AWS untuk menghubungi hingga tiga kontak alternatif yang terkait dengan akun. Kontak alternatif tidak harus menjadi orang tertentu. Sebagai gantinya, Anda dapat menambahkan daftar distribusi email jika Anda memiliki tim yang mengelola masalah terkait penagihan, operasi, dan keamanan. Ini adalah tambahan untuk alamat email yang terkait dengan [pengguna root](#) akun. [Kontak akun utama](#) akan terus menerima semua komunikasi email yang dikirim ke email akun root.

Anda hanya dapat menentukan satu dari masing-masing jenis kontak berikut yang terkait dengan akun.

- Kontak penagihan
- Kontak operasi
- Kontak keamanan

Anda dapat menambahkan atau mengedit kontak alternatif secara berbeda, tergantung pada apakah akun berdiri sendiri atau tidak, atau bagian dari organisasi:

- **Mandiri Akun AWS** — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui kontak alternatif Anda sendiri menggunakan Konsol AWS Manajemen, atau melalui AWS CLI & SDK. Untuk mempelajari cara melakukannya, lihat [Memperbarui kontak alternatif untuk mandiri Akun AWS](#).
- **Akun AWS dalam organisasi** — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui akun anggota apa pun di organisasi secara terpusat dari AWS Organizations konsol, atau secara terprogram melalui CLI AWS & SDK. Untuk mempelajari cara melakukannya, lihat [Memperbarui kontak alternatif untuk setiap kontak Akun AWS di organisasi Anda](#).

Topik

- [Persyaratan nomor telepon dan alamat email](#)
- [Perbarui kontak alternatif untuk mandiri Akun AWS](#)
- [Perbarui kontak alternatif untuk apa pun Akun AWS di organisasi Anda](#)
- [akun: kunci AlternateContactTypes konteks](#)

Persyaratan nomor telepon dan alamat email

Sebelum Anda melanjutkan dengan memperbarui informasi kontak alternatif akun Anda, kami sarankan Anda terlebih dahulu meninjau persyaratan berikut saat memasukkan nomor telepon dan alamat email.

- Nomor telepon hanya dapat berisi angka, spasi putih, dan karakter berikut: "" . + - ()
- Alamat email dapat mencapai 254 karakter dan dapat menyertakan karakter khusus berikut di bagian lokal alamat email selain yang alfanumerik standar: "" . += . # | ! & - _

Perbarui kontak alternatif untuk mandiri Akun AWS

Untuk menambah atau mengedit kontak alternatif untuk mandiri Akun AWS, lakukan langkah-langkah dalam prosedur berikut. Konsol Manajemen AWS Prosedur di bawah ini selalu berfungsi hanya dalam konteks mandiri. Anda dapat menggunakan Konsol Manajemen AWS untuk mengakses atau mengubah hanya kontak alternatif di akun yang Anda gunakan untuk memanggil operasi.

Konsol Manajemen AWS

Untuk menambah atau mengedit kontak alternatif untuk mandiri Akun AWS

Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- `account:GetAlternateContact`(untuk melihat rincian kontak alternatif)
- `account:PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
- `account>DeleteAlternateContact`(untuk menghapus kontak alternatif)

1. Masuk ke [Konsol Manajemen AWS](#) sebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Pada [halaman Akun](#), gulir ke bawah ke Kontak alternatif, dan di sebelah kanan judul, pilih Edit.

Note

Jika Anda tidak melihat opsi Edit, kemungkinan Anda tidak masuk sebagai pengguna root untuk akun Anda atau sebagai seseorang yang memiliki izin minimum yang ditentukan di atas.

4. Ubah nilai di salah satu bidang yang tersedia.

Important

Untuk bisnis Akun AWS, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada satu milik individu.

5. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak alternatif dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

Catatan

- Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus [mengaktifkan akses tepercaya untuk layanan Akun](#).

Izin minimum

Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:

- `GetAlternateContact`(untuk melihat rincian kontak alternatif)
- `PutAlternateContact`(untuk mengatur atau memperbarui kontak alternatif)
- `DeleteAlternateContact`(untuk menghapus kontak alternatif)

Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil kontak alternatif Penagihan saat ini untuk akun pemanggil.

```
$ aws account get-alternate-contact \
```

```
--alternate-contact-type=BILLING
{
  "AlternateContact": {
    "AlternateContactType": "BILLING",
    "EmailAddress": "saanvi.sarkar@amazon.com",
    "Name": "Saanvi Sarkar",
    "PhoneNumber": "+1(206)555-0123",
    "Title": "CF0"
  }
}
```

Example

Contoh berikut menetapkan kontak alternatif Operasi baru untuk akun pemanggil.

```
$ aws account put-alternate-contact \
  --alternate-contact-type=OPERATIONS \
  --email-address=mateo_jackson@amazon.com \
  --name="Mateo Jackson" \
  --phone-number="+1(206)555-1234" \
  --title="Operations Manager"
```

Perintah ini tidak menghasilkan output jika berhasil.

Example

Note

Jika Anda melakukan beberapa `PutAlternateContact` operasi pada jenis kontak yang sama Akun AWS dan sama, yang pertama menambahkan kontak baru, dan semua panggilan berturut-turut ke jenis kontak yang sama Akun AWS dan memperbarui kontak yang ada.

Example

Contoh berikut menghapus kontak alternatif Keamanan untuk akun pemanggil.

```
$ aws account delete-alternate-contact \
  --alternate-contact-type=SECURITY
```

Perintah ini tidak menghasilkan output jika berhasil.

Note

Jika Anda mencoba menghapus kontak yang sama lebih dari sekali, yang pertama berhasil diam-diam. Semua upaya selanjutnya menghasilkan ResourceNotFound pengecualian.

Perbarui kontak alternatif untuk apa pun Akun AWS di organisasi Anda

Untuk menambah atau mengedit rincian kontak alternatif untuk setiap orang Akun AWS di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan

Untuk memperbarui kontak alternatif dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat [Mengaktifkan semua fitur untuk](#) organisasi.
- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihat [Aktifkan akses tepercaya untuk AWS Pengelolaan Akun](#).

Note

Kebijakan AWS Organizations terkelola `AWSOrganizationsReadOnlyAccess` atau `AWSOrganizationsFullAccess` diperbarui untuk memberikan izin mengakses API Manajemen AWS Akun sehingga Anda dapat mengakses data akun dari AWS Organizations konsol. Untuk melihat kebijakan terkelola yang diperbarui, lihat Kebijakan yang [AWS dikelola Update to Organizations](#).

Konsol Manajemen AWS

Untuk menambah atau mengedit kontak alternatif untuk setiap Akun AWS di organisasi Anda

1. Masuk ke [AWS Organizations konsol](#) dengan kredensial akun manajemen organisasi.

2. Dari Akun AWS, pilih akun yang ingin Anda perbarui.
3. Pilih Info kontak, dan di bawah Kontak alternatif, cari jenis kontak: Kontak penagihan, Kontak keamanan, atau Kontak operasi.
4. Untuk menambahkan kontak baru, pilih Tambah, atau untuk memperbarui kontak yang ada pilih Edit.
5. Ubah nilai di salah satu bidang yang tersedia.

 Important

Untuk bisnis Akun AWS, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada satu milik individu.

6. Setelah Anda membuat semua perubahan, pilih Perbarui.


AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak alternatif dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- [GetAlternateContact](#)
- [PutAlternateContact](#)
- [DeleteAlternateContact](#)

 Catatan

- Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus [mengaktifkan akses tepercaya untuk layanan Akun](#).
- Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

 Izin minimum

Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:


```
--alternate-contact-type=OPERATIONS \  
--email-address=mateo_jackson@amazon.com \  
--name="Mateo Jackson" \  
--phone-number="+1(206)555-1234" \  
--title="Operations Manager"
```

Perintah ini tidak menghasilkan output jika berhasil.

Note

Jika Anda melakukan beberapa `PutAlternateContact` operasi pada jenis kontak yang sama Akun AWS dan sama, yang pertama menambahkan kontak baru, dan semua panggilan berturut-turut ke jenis kontak yang sama Akun AWS dan memperbarui kontak yang ada.

Example

Contoh berikut menghapus kontak alternatif Keamanan untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account delete-alternate-contact \  
--account-id 123456789012 \  
--alternate-contact-type=SECURITY
```

Perintah ini tidak menghasilkan output jika berhasil.

Example

Note

Jika Anda mencoba menghapus kontak yang sama lebih dari sekali, yang pertama berhasil diam-diam. Semua upaya selanjutnya menghasilkan `ResourceNotFound` pengecualian.

akun: kunci AlternateContactTypes konteks

Anda dapat menggunakan kunci konteks `account:AlternateContactTypes` untuk menentukan mana dari tiga jenis kontak yang diizinkan (atau ditolak) oleh kebijakan IAM. Misalnya, contoh kebijakan izin IAM berikut menggunakan kunci kondisi ini untuk mengizinkan prinsipal terlampir mengambil, tetapi tidak memodifikasi, hanya kontak BILLING alternatif untuk akun tertentu dalam organisasi.

Karena `account:AlternateContactTypes` adalah jenis string multi-nilai, Anda harus menggunakan [ForAnyValue atau ForAllValues multi-nilai operator string](#).

Perbarui kontak utama untuk Anda Akun AWS

Anda dapat memperbarui informasi kontak utama yang terkait dengan akun Anda, termasuk nama lengkap kontak Anda, nama perusahaan, alamat surat, nomor telepon, dan alamat situs web.

Anda mengedit kontak akun utama secara berbeda, tergantung pada apakah akun tersebut berdiri sendiri, atau bagian dari organisasi:

- **Mandiri Akun AWS** — Untuk Akun AWS tidak terkait dengan organisasi, Anda dapat memperbarui kontak akun utama Anda sendiri menggunakan Konsol AWS Manajemen, atau melalui AWS CLI & SDK. Untuk mempelajari cara melakukannya, lihat [Memperbarui kontak Akun AWS utama mandiri](#).
- **Akun AWS dalam organisasi** — Untuk akun anggota yang merupakan bagian dari AWS organisasi, pengguna di akun manajemen atau akun admin yang didelegasikan dapat memperbarui akun anggota apa pun di organisasi secara terpusat dari AWS Organizations konsol, atau secara terprogram melalui CLI AWS & SDK. Untuk mempelajari cara melakukannya, lihat [Memperbarui kontak Akun AWS utama di organisasi Anda](#).

Topik

- [Persyaratan nomor telepon dan alamat email](#)
- [Perbarui kontak utama untuk standalone Akun AWS atau akun manajemen](#)
- [Perbarui kontak utama untuk apa pun AWS akun anggota di organisasi Anda](#)

Persyaratan nomor telepon dan alamat email

Sebelum Anda melanjutkan dengan memperbarui informasi kontak utama akun Anda, kami sarankan Anda terlebih dahulu meninjau persyaratan berikut saat memasukkan nomor telepon dan alamat email.

- Nomor telepon seharusnya hanya berisi angka.
- Nomor telepon harus dimulai dengan kode + dan negara dan tidak boleh memiliki nol di depan atau spasi tambahan setelah kode negara. Misalnya, +1 (US/Canada) atau +44 (Inggris).
- Nomor telepon tidak boleh menyertakan spasi antara kode area, kode pertukaran, dan kode lokal. Misalnya, +12025550179.
- Untuk tujuan keamanan, nomor telepon harus mampu menerima SMS dari AWS. Nomor bebas pulsa tidak akan diterima karena sebagian besar tidak mendukung SMS.
- Untuk bisnis Akun AWS, itu adalah praktik terbaik untuk memasukkan nomor telepon perusahaan dan alamat email daripada satu milik individu. Mengkonfigurasi [pengguna root](#) akun dengan alamat email atau nomor telepon individu dapat membuat akun Anda sulit dipulihkan jika individu tersebut meninggalkan perusahaan.

Perbarui kontak utama untuk standalone Akun AWS atau akun manajemen

Untuk mengedit detail kontak utama Anda untuk mandiri Akun AWS, lakukan langkah-langkah dalam prosedur berikut. Konsol Manajemen AWS Prosedur di bawah ini selalu berfungsi hanya dalam konteks mandiri. Anda dapat menggunakan Konsol Manajemen AWS untuk mengakses atau mengubah hanya informasi kontak utama dari akun yang Anda gunakan untuk memanggil operasi.

Konsol Manajemen AWS

Untuk mengedit kontak utama Anda untuk standalone Akun AWS

Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- `account:GetContactInformation`(untuk melihat detail kontak utama)

- `account:PutContactInformation`(untuk memperbarui detail kontak utama)

1. Masuk ke [Konsol Manajemen AWS](#) sebagai pengguna IAM atau peran yang memiliki izin minimum.
2. Pilih nama akun Anda di kanan atas jendela, lalu pilih Akun.
3. Gulir ke bawah ke bagian Informasi kontak, dan di sebelahnya pilih Edit.
4. Ubah nilai di salah satu bidang yang tersedia.
5. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak utama dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- [GetContactInformation](#)
- [PutContactInformation](#)

Catatan

- Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus [mengaktifkan akses tepercaya untuk layanan Akun](#).

Izin minimum

Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:

- `account:GetContactInformation`
- `account:PutContactInformation`

Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil informasi kontak utama saat ini untuk akun pemanggil.

```
$ aws account get-contact-information
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
    "StateOrRegion": "WA",
    "WebsiteUrl": "https://www.examplecorp.com"
  }
}
```

Example

Contoh berikut menetapkan informasi kontak utama baru untuk akun pemanggil.

```
$ aws account put-contact-information --contact-information \
'{"AddressLine1": "123 Any Street", "City": "Seattle", "CompanyName": "Example Corp,
Inc.", "CountryCode": "US", "DistrictOrCounty": "King",
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Perintah ini tidak menghasilkan output jika berhasil.

Perbarui kontak utama untuk apa pun AWS akun anggota di organisasi Anda

Untuk mengedit detail kontak utama Anda di akun AWS anggota mana pun di organisasi Anda, lakukan langkah-langkah dalam prosedur berikut.

Persyaratan tambahan

Untuk memperbarui kontak utama dengan AWS Organizations konsol, Anda perlu melakukan beberapa pengaturan awal:

- Organisasi Anda harus mengaktifkan semua fitur untuk mengelola pengaturan pada akun anggota Anda. Ini memungkinkan kontrol admin atas akun anggota. Ini diatur secara default saat Anda membuat organisasi. Jika organisasi Anda disetel ke penagihan gabungan saja, dan Anda ingin mengaktifkan semua fitur, lihat [Mengaktifkan semua fitur untuk organisasi](#).
- Anda perlu mengaktifkan akses tepercaya untuk layanan Manajemen AWS Akun. Untuk mengatur ini, lihat [Aktifkan akses tepercaya untuk AWS Pengelolaan Akun](#).

Konsol Manajemen AWS

Untuk mengedit kontak utama Anda untuk setiap Akun AWS di organisasi Anda

1. Masuk ke [AWS Organizations konsol](#) dengan kredensial akun manajemen organisasi.
2. Dari Akun AWS, pilih akun yang ingin Anda perbarui.
3. Pilih Info kontak, dan temukan Kontak utama,
4. Pilih Edit.
5. Ubah nilai di salah satu bidang yang tersedia.
6. Setelah Anda membuat semua perubahan, pilih Perbarui.

AWS CLI & SDKs

Anda dapat mengambil, memperbarui, atau menghapus informasi kontak utama dengan menggunakan AWS CLI perintah berikut atau operasi setara AWS SDK mereka:

- [GetContactInformation](#)
- [PutContactInformation](#)

Catatan

- Untuk melakukan operasi ini dari akun manajemen atau akun admin yang didelegasikan di organisasi terhadap akun anggota, Anda harus [mengaktifkan akses tepercaya untuk layanan Akun](#).
- Anda tidak dapat mengakses akun di organisasi yang berbeda dari yang Anda gunakan untuk memanggil operasi.

Izin minimum

Untuk setiap operasi, Anda harus memiliki izin yang memetakan ke operasi itu:

- `account:GetContactInformation`
- `account:PutContactInformation`

Jika Anda menggunakan izin individual ini, Anda dapat memberikan beberapa pengguna kemampuan untuk hanya membaca informasi kontak, dan memberi orang lain kemampuan untuk membaca dan menulis.

Example

Contoh berikut mengambil informasi kontak utama saat ini untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account get-contact-information --account-id 123456789012
{
  "ContactInformation": {
    "AddressLine1": "123 Any Street",
    "City": "Seattle",
    "CompanyName": "Example Corp, Inc.",
    "CountryCode": "US",
    "DistrictOrCounty": "King",
    "FullName": "Saanvi Sarkar",
    "PhoneNumber": "+15555550100",
    "PostalCode": "98101",
```

```
    "StateOrRegion": "WA",  
    "WebsiteUrl": "https://www.examplecorp.com"  
  }  
}
```

Example

Contoh berikut menetapkan informasi kontak utama untuk akun anggota yang ditentukan dalam suatu organisasi. Kredensi yang digunakan harus berasal dari akun manajemen organisasi, atau dari akun admin yang didelegasikan oleh Manajemen Akun.

```
$ aws account put-contact-information --account-id 123456789012 \  
--contact-information '{"AddressLine1": "123 Any Street", "City": "Seattle",  
"CompanyName": "Example Corp, Inc.", "CountryCode": "US", "DistrictOrCounty":  
"King",  
"FullName": "Saanvi Sarkar", "PhoneNumber": "+15555550100", "PostalCode": "98101",  
"StateOrRegion": "WA", "WebsiteUrl": "https://www.examplecorp.com"}'
```

Perintah ini tidak menghasilkan output jika berhasil.

Tampilan Akun AWS pengidentifikasi

AWS menetapkan pengidentifikasi unik berikut untuk masing-masing: Akun AWS

[Akun AWS ID](#)

Angka 12 digit, seperti 012345678901, yang secara unik mengidentifikasi sebuah Akun AWS. Banyak AWS sumber daya menyertakan ID akun di [Amazon Resource Names \(ARN\)](#) mereka. Bagian ID akun membedakan sumber daya dalam satu akun dari sumber daya di akun lain. Jika Anda adalah pengguna AWS Identity and Access Management (IAM), Anda dapat masuk Konsol Manajemen AWS menggunakan ID akun atau alias akun. Meskipun ID akun, seperti informasi pengenalan apa pun, harus digunakan dan dibagikan dengan hati-hati, ID tersebut tidak dianggap sebagai informasi rahasia, sensitif, atau rahasia.

[ID pengguna kanonik](#)

Pengidentifikasi alfa-numerik, seperti 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be, yang merupakan bentuk ID yang dikaburkan. Akun AWS Anda dapat menggunakan ID ini

untuk mengidentifikasi Akun AWS saat memberikan akses lintas akun ke bucket dan objek menggunakan Amazon Simple Storage Service (Amazon S3). Anda dapat mengambil ID pengguna kanonik untuk Anda Akun AWS sebagai pengguna [root atau pengguna IAM](#).

Anda harus diautentikasi dengan AWS untuk melihat pengidentifikasi ini.

Warning

Jangan berikan AWS kredensi Anda (termasuk kata sandi dan kunci akses) kepada pihak ketiga yang membutuhkan Akun AWS pengenalan Anda untuk berbagi AWS sumber daya dengan Anda. Melakukan hal itu akan memberi mereka akses yang sama ke Akun AWS yang Anda miliki.

Temukan Anda Akun AWS ID

Anda dapat menemukan Akun AWS ID menggunakan salah satu Konsol Manajemen AWS atau AWS Command Line Interface (AWS CLI). Di konsol, lokasi ID akun tergantung pada apakah Anda masuk sebagai pengguna root atau pengguna IAM. ID akun sama apakah Anda masuk sebagai pengguna root atau pengguna IAM.

Menemukan ID akun Anda sebagai pengguna root

Konsol Manajemen AWS

Untuk menemukan Akun AWS ID saat masuk sebagai pengguna root

Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- Saat Anda masuk sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.

1. Di bilah navigasi di kanan atas, pilih nama atau nomor akun Anda, lalu pilih Kredensi keamanan.

i Tip

Jika Anda tidak melihat opsi Security credentials, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

2. Di bagian Detail akun, nomor akun muncul di sebelah Akun AWS ID.

AWS CLI & SDKs

Untuk menemukan Akun AWS ID Anda menggunakan AWS CLI

i Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- Saat Anda menjalankan perintah sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.

Gunakan perintah [get-caller-identity](#) sebagai berikut.

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text  
123456789012
```

Temukan ID akun Anda sebagai pengguna IAM

Konsol Manajemen AWS

Untuk menemukan Akun AWS ID saat masuk sebagai pengguna IAM

i Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- `account:GetAccountInformation`

1. Di bilah navigasi di kanan atas, pilih nama pengguna Anda dan kemudian pilih Kredensi keamanan.

i Tip

Jika Anda tidak melihat opsi Security credentials, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

2. Di bagian atas halaman, di bawah Detail akun, nomor akun muncul di sebelah Akun AWS ID.

AWS CLI & SDKs

Untuk menemukan Akun AWS ID Anda menggunakan AWS CLI

i Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- Ketika Anda menjalankan perintah sebagai pengguna atau peran IAM, maka Anda harus memiliki:
 - `sts:GetCallerIdentity`

Gunakan perintah [get-caller-identity](#) sebagai berikut.

```
$ aws sts get-caller-identity \  
  --query Account \  
  --output text  
123456789012
```

Temukan ID pengguna kanonik untuk Anda Akun AWS

Anda dapat menemukan ID pengguna kanonik untuk Anda Akun AWS menggunakan Konsol Manajemen AWS atau AWS CLI ID pengguna kanonik untuk akun khusus untuk akun Akun AWS itu. Anda dapat mengambil ID pengguna kanonik untuk Anda Akun AWS sebagai pengguna root, pengguna federasi, atau pengguna IAM.

Temukan ID kanonik sebagai pengguna root atau pengguna IAM

Konsol Manajemen AWS

Untuk menemukan ID pengguna kanonik untuk akun Anda saat masuk ke konsol sebagai pengguna root atau pengguna IAM

Izin minimum

Untuk melakukan langkah-langkah berikut, Anda harus memiliki setidaknya izin IAM berikut:

- Saat Anda menjalankan perintah sebagai pengguna root, Anda tidak memerlukan izin IAM apa pun.
- Ketika Anda masuk sebagai pengguna IAM, maka Anda harus memiliki:
 - `account:GetAccountInformation`

1. Masuk ke Konsol Manajemen AWS sebagai pengguna root atau pengguna IAM.
2. Di bilah navigasi di kanan atas, pilih nama atau nomor akun Anda, lalu pilih Kredensi keamanan.

Tip

Jika Anda tidak melihat opsi Security credentials, Anda mungkin masuk sebagai pengguna federasi dengan peran IAM, bukan sebagai pengguna IAM. Dalam hal ini, cari entri Akun dan nomor ID akun di sebelahnya.

3. Di bagian Detail akun, ID pengguna kanonik muncul di sebelah ID pengguna Canonical. Anda dapat menggunakan ID pengguna kanonik untuk mengonfigurasi daftar kontrol akses Amazon S3 (ACL).

AWS CLI & SDKs

Untuk menemukan ID pengguna kanonik menggunakan AWS CLI

Perintah yang sama AWS CLI dan API berfungsi untuk Pengguna root akun AWS, pengguna IAM, atau peran IAM.

Gunakan perintah [list-buckets](#) sebagai berikut.

```
$ aws s3api list-buckets \
  --max-items 10 \
  --page-size 10 \
  --query Owner.ID \
  --output text
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Temukan ID kanonik sebagai pengguna federasi dengan peran IAM

Konsol Manajemen AWS

Untuk menemukan ID kanonik untuk akun Anda saat masuk ke konsol sebagai pengguna gabungan dengan peran IAM

Izin minimum

- Anda harus memiliki izin untuk mendaftar dan melihat bucket Amazon S3.

1. Masuk ke Konsol Manajemen AWS sebagai pengguna federasi dengan peran IAM.
2. Di konsol Amazon S3, pilih nama bucket untuk melihat detail tentang bucket.
3. Pilih tab Izin.
4. Di bagian Daftar kontrol akses, di bawah Pemilik Bucket, ID kanonik untuk Anda Akun AWS akan muncul.

AWS CLI & SDKs

Untuk menemukan ID pengguna kanonik menggunakan AWS CLI

Perintah yang sama AWS CLI dan API berfungsi untuk Pengguna root akun AWS, pengguna IAM, atau peran IAM.

Gunakan perintah [list-buckets](#) sebagai berikut.

```
$ aws s3api list-buckets \  
  --max-items 10 \  
  --page-size 10 \  
  --query Owner.ID \  
  --output text  
249fa2f1dc32c330EXAMPLE91b2778fcc65f980f9172f9cb9a5f50ccbEXAMPLE
```

Keamanan di AWS Pengelolaan Akun

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program Kepatuhan Program [AWS Kepatuhan Program AWS](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Manajemen Akun, lihat [Layanan AWS cakupan berdasarkan program kepatuhan Layanan AWS](#) .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Manajemen AWS Akun. Ini menunjukkan kepada Anda cara mengonfigurasi Manajemen Akun untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Manajemen Akun Anda.

Topik

- [Perlindungan data di AWS Pengelolaan Akun](#)
- [AWS PrivateLink untuk AWS Pengelolaan Akun](#)
- [Identity and Access Management untuk AWS Pengelolaan Akun](#)
- [AWS kebijakan terkelola untuk Manajemen AWS Akun](#)
- [Validasi kepatuhan untuk Manajemen AWS Akun](#)
- [Ketahanan dalam Manajemen Akun AWS](#)
- [Keamanan infrastruktur di AWS Account Management](#)

Perlindungan data di AWS Pengelolaan Akun

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data dalam Manajemen AWS Akun. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [FAQ Privasi Data AWS](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Pusat Peraturan Perlindungan Data Umum \(GDPR\)](#).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensi dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan logging aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Manajemen Akun atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

AWS PrivateLink untuk AWS Pengelolaan Akun

Jika Anda menggunakan Amazon Virtual Private Cloud (Amazon VPC) untuk meng-host AWS sumber daya Anda, Anda dapat mengakses layanan Manajemen AWS Akun dari dalam VPC tanpa harus melintasi internet publik.

Amazon VPC memungkinkan Anda meluncurkan AWS sumber daya di jaringan virtual khusus. Anda dapat menggunakan VPC untuk mengendalikan pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan. Untuk informasi lebih lanjut tentang Amazon VPC, lihat [Panduan Pengguna Amazon VPC](#).

Untuk menghubungkan VPC Amazon Anda ke Manajemen Akun, Anda harus terlebih dahulu menentukan titik akhir VPC antarmuka, yang memungkinkan Anda menghubungkan VPC Anda ke layanan lain. AWS Titik akhir memberikan konektivitas yang dapat andal, dapat diskalakan, tanpa memerlukan gateway internet, instans terjemahan alamat jaringan (NAT), atau koneksi VPN. Untuk informasi selengkapnya, lihat [VPC Endpoint Antarmuka \(AWS PrivateLink\)](#) dalam Panduan Pengguna Amazon VPC.

Membuat Titik Akhir

Anda dapat membuat titik akhir Manajemen AWS Akun di VPC menggunakan Konsol Manajemen AWS, AWS CLI(), AWS Command Line Interface SDK, AWS API Manajemen Akun, AWS atau CloudFormation

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan konsol VPC Amazon atau AWS CLI, lihat [Membuat Titik Akhir Antarmuka di Panduan Pengguna Amazon VPC](#).

Note

Saat Anda membuat titik akhir, tentukan Manajemen Akun sebagai layanan yang Anda inginkan untuk disambungkan oleh VPC, menggunakan format berikut:

```
com.amazonaws.us-east-1.account
```

Anda harus menggunakan string persis seperti yang ditunjukkan, menentukan us-east-1 Wilayah. Sebagai layanan global, Manajemen Akun hanya dihosting di satu AWS Wilayah itu.

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan CloudFormation, lihat sumber daya [AWS: :EC2: :vpcendPoint](#) di Panduan Pengguna.CloudFormation

Kebijakan Amazon VPC Endpoint

Anda dapat mengontrol tindakan apa yang dapat dilakukan melalui titik akhir layanan ini dengan melampirkan kebijakan titik akhir saat Anda membuat titik akhir VPC Amazon. Anda dapat membuat aturan IAM kompleks dengan melampirkan beberapa kebijakan titik akhir. Untuk informasi lebih lanjut, lihat:

- [Kebijakan endpoint Amazon Virtual Private Cloud untuk Manajemen Akun](#)
- [Mengontrol Akses ke Layanan dengan Titik Akhir VPC dalam Panduan.AWS PrivateLink](#)

Kebijakan endpoint Amazon Virtual Private Cloud untuk Manajemen Akun

Anda dapat membuat kebijakan titik akhir VPC Amazon untuk Manajemen Akun di mana Anda menentukan hal berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan oleh kepala sekolah.
- Sumber daya untuk melakukan tindakan.

Contoh berikut menunjukkan kebijakan titik akhir VPC Amazon yang memungkinkan satu pengguna IAM bernama Alice di akun 123456789012 untuk mengambil dan mengubah informasi kontak alternatif untuk apa pun Akun AWS, tetapi menolak semua izin pengguna IAM untuk menghapus informasi kontak alternatif apa pun di akun apa pun.

Jika Anda ingin memberikan akses ke akun yang merupakan bagian dari AWS Organisasi kepada prinsipal yang ada di salah satu akun anggota organisasi, maka Resource elemen tersebut harus menggunakan format berikut:

```
arn:aws:account::{ManagementAccountId}:account/o-{OrganizationId}/{AccountId}
```

Untuk informasi selengkapnya tentang membuat kebijakan titik akhir, lihat [Mengontrol Akses ke Layanan dengan Titik Akhir VPC](#) di Panduan.AWS PrivateLink

Identity and Access Management untuk AWS Pengelolaan Akun

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Manajemen Akun. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana AWS Manajemen Akun bekerja dengan IAM](#)
- [Identity-based contoh kebijakan untuk AWS Pengelolaan Akun](#)
- [Menggunakan kebijakan berbasis identitas \(kebijakan IAM\) untuk AWS Pengelolaan Akun](#)
- [Pemecahan masalah AWS Identitas dan akses Manajemen Akun](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Pemecahan masalah AWS Identitas dan akses Manajemen Akun](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana AWS Manajemen Akun bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Identity-based contoh kebijakan untuk AWS Pengelolaan Akun](#))

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensi dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk

informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh

identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat [Pilih antara kebijakan terkelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCP\)](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana AWS Manajemen Akun bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Manajemen Akun, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Manajemen Akun.

Fitur IAM yang dapat Anda gunakan AWS Pengelolaan Akun

Fitur IAM	Dukungan Manajemen Akun
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Tidak
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Tidak
Service-linked peran	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Manajemen Akun dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Identity-based kebijakan untuk Manajemen Akun

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan](#) dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat [Referensi elemen kebijakan JSON IAM](#) dalam Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk Manajemen Akun

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat [Identity-based contoh kebijakan untuk AWS Pengelolaan Akun](#)

Resource-based kebijakan dalam Manajemen Akun

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Manajemen Akun

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Manajemen Akun, lihat [Tindakan yang ditentukan oleh Manajemen AWS Akun](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan dalam Manajemen Akun menggunakan awalan berikut sebelum tindakan.

```
account
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [  
  "account:action1",  
  "account:action2"  
]
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang bekerja dengan kontak alternatif Akun AWS seseorang, sertakan tindakan berikut.

```
"Action": "account:*AlternateContact"
```

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat [Identity-based contoh kebijakan untuk AWS Pengelolaan Akun](#)

Sumber daya kebijakan untuk Manajemen Akun

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"

```

Layanan Manajemen Akun mendukung jenis sumber daya spesifik berikut dalam `Resource` elemen kebijakan IAM untuk membantu Anda memfilter kebijakan dan membedakan antara jenis Akun AWS berikut:

- akun

`resource`Jenis ini hanya cocok dengan akun mandiri Akun AWS yang bukan akun anggota dalam organisasi yang dikelola oleh AWS Organizations layanan.

- akun InOrganization

`resource`Jenis ini hanya Akun AWS cocok dengan akun anggota dalam organisasi yang dikelola oleh AWS Organizations layanan.

Untuk melihat daftar jenis sumber daya Manajemen Akun dan ARNnya, lihat [Sumber daya yang ditentukan oleh Manajemen AWS Akun](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh Manajemen AWS Akun](#).

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat. [Identity-based contoh kebijakan untuk AWS Pengelolaan Akun](#)

Kunci kondisi kebijakan untuk Manajemen Akun

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang

diminta. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Layanan Manajemen Akun mendukung kunci kondisi berikut yang dapat Anda gunakan untuk memberikan pemfilteran halus untuk kebijakan IAM Anda:

- akun: TargetRegion

Kunci kondisi ini mengambil argumen yang terdiri dari daftar [kode AWS Wilayah](#). Ini memungkinkan Anda memfilter kebijakan agar hanya memengaruhi tindakan yang berlaku pada Wilayah tertentu.

- akun: AlternateContactTypes

Kunci kondisi ini mengambil daftar jenis kontak alternatif:

- PENAGIHAN
- OPERASI
- SEKURITI

Menggunakan kunci ini memungkinkan Anda memfilter permintaan hanya untuk tindakan yang menargetkan jenis kontak alternatif yang ditentukan.

- akun: AccountResourceOrgPaths

Kunci kondisi ini mengambil argumen yang terdiri dari daftar jalur melalui hierarki organisasi Anda ke unit organisasi tertentu (OU). Ini memungkinkan Anda memfilter kebijakan untuk hanya memengaruhi akun target di OU yang cocok.

```
o-aa111bb222/r-a1b2/ou-a1b2-f6g7h111/*
```

- akun: AccountResourceOrgTags

Kunci kondisi ini mengambil argumen yang terdiri dari daftar kunci tag dan nilai. Ini memungkinkan Anda memfilter kebijakan untuk hanya memengaruhi akun yang merupakan anggota organisasi dan yang ditandai dengan kunci dan nilai tag yang ditentukan.

- akun: EmailTargetDomain

Kunci kondisi ini mengambil argumen yang terdiri dari daftar domain email. Ini memungkinkan Anda memfilter kebijakan agar hanya memengaruhi tindakan yang cocok dengan domain email yang ditentukan. Kunci kondisi ini peka huruf besar/kecil. Anda harus menggunakan `StringEqualsIgnoreCase` alih-alih `StringEquals` di blok kondisi kebijakan untuk

mengontrol tindakan berdasarkan domain alamat email target. Berikut adalah contoh kebijakan yang memungkinkan `account:StartPrimaryEmailUpdate` tindakan untuk diselesaikan ketika domain email berisi `example.com`, `company.org`, atau kombinasi kasus apa pun, seperti `EXAMPLE.COM`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowConditionKey",
      "Effect": "Allow",
      "Action": [
        "account:StartPrimaryEmailUpdate"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "account:EmailTargetDomain": [
            "example.com",
            "company.org"
          ]
        }
      }
    }
  ]
}
```

Untuk melihat daftar kunci kondisi Manajemen Akun, lihat [Kunci kondisi untuk Manajemen AWS Akun](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh Manajemen AWS Akun](#).

Untuk melihat contoh kebijakan berbasis identitas Manajemen Akun, lihat [Identity-based contoh kebijakan untuk AWS Pengelolaan Akun](#)

Daftar kontrol akses di Manajemen Akun

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Attribute-based kontrol akses dengan Manajemen Akun

Mendukung ABAC (tag dalam kebijakan): Tidak

Attribute-based Access Control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik principal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk Manajemen AWS Akun, kontrol akses berbasis tag hanya didukung melalui kunci `account:AccountResourceOrgTags/key-name` kondisi. Kunci `aws:ResourceTag/key-name` kondisi standar tidak didukung untuk API di namespace akun.

Contoh kebijakan JSON menggunakan kunci kondisi yang didukung

Contoh kebijakan berikut memungkinkan akses untuk melihat informasi kontak untuk akun yang ditandai dengan kunci "" dan nilai "CostCenter12345" atau "67890" di organisasi Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "account:GetContactInformation",
        "account:GetAlternateContact"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "account:AccountResourceOrgTags/CostCenter": [
            "12345",
            "67890"
          ]
        }
      }
    }
  ]
}
```

```
}  
  ]  
}
```

Untuk informasi selengkapnya tentang ABAC, lihat [Mendefinisikan izin berdasarkan atribut dengan otorisasi ABAC](#) dan [tutorial IAM: Menentukan izin untuk mengakses AWS sumber daya berdasarkan tag di Panduan Pengguna IAM](#).

Menggunakan kredensial sementara dengan Manajemen Akun

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

Cross-service izin utama untuk Manajemen Akun

Mendukung sesi akses terusan (FAS): Ya

Sesi akses terusan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

Peran layanan untuk Manajemen Akun

Mendukung peran layanan: Tidak

Peran layanan adalah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Service-linked peran untuk Manajemen Akun

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke Layanan AWS. Layanan AWS dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda

Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat [Layanan AWS yang berfungsi dengan IAM](#). Temukan layanan dalam tabel yang Yes menyertakan kolom Service-linked peran. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Identity-based contoh kebijakan untuk AWS Pengelolaan Akun

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau mengubah sumber daya Manajemen Akun. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM \(konsol\) di Panduan Pengguna IAM](#).

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Manajemen Akun, termasuk format ARN untuk setiap jenis sumber daya, lihat [Tindakan, sumber daya, dan kunci kondisi untuk Manajemen AWS Akun](#) dalam Referensi Otorisasi Layanan.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan halaman Akun di Konsol Manajemen AWS](#)
- [Menyediakan akses hanya-baca ke halaman Akun di Konsol Manajemen AWS](#)
- [Memberikan akses penuh ke halaman Akun di Konsol Manajemen AWS](#)

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Manajemen Akun di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi

selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan halaman Akun di Konsol Manajemen AWS

Untuk mengakses [halaman Akun](#) di Konsol Manajemen AWS, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang

diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa pengguna dan peran dapat menggunakan konsol Manajemen Akun, Anda dapat memilih untuk melampirkan kebijakan `AWSAccountManagementReadOnlyAccess` atau `AWSAccountManagementFullAccess` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, dalam banyak kasus, Anda dapat memilih untuk mengizinkan akses hanya ke tindakan yang cocok dengan operasi API yang Anda coba lakukan.

Menyediakan akses hanya-baca ke halaman Akun di Konsol Manajemen AWS

Dalam contoh berikut, Anda ingin memberikan pengguna IAM di akses Akun AWS hanya-baca ke halaman Akun di halaman. Konsol Manajemen AWS Pengguna dengan kebijakan ini terlampir tidak dapat melakukan perubahan apa pun.

`account:GetAccountInformation` tindakan memberikan akses untuk melihat sebagian besar pengaturan di halaman Akun. Namun, untuk melihat AWS Wilayah yang saat ini diaktifkan, Anda juga harus menyertakan `account:ListRegions` tindakan.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantReadOnlyAccessToAccountSettings",
      "Effect": "Allow",
      "Action": [
        "account:GetAccountInformation",
        "account:ListRegions"
      ],
      "Resource": "*"
    }
  ]
}
```

Memberikan akses penuh ke halaman Akun di Konsol Manajemen AWS

Dalam contoh berikut, Anda ingin memberikan pengguna IAM dalam akses Akun AWS penuh Anda ke halaman Akun di Konsol Manajemen AWS. Pengguna dengan kebijakan ini terlampir dapat mengubah pengaturan untuk akun.

Kebijakan contoh ini dibuat berdasarkan kebijakan contoh sebelumnya dengan menambahkan setiap izin tulis yang tersedia (kecuali CloseAccount), yang memungkinkan pengguna mengubah sebagian besar pengaturan untuk akun, termasuk izin dan izin. `account:EnableRegion`
`account:DisableRegion`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantFullAccessToAccountSettings",
      "Effect": "Allow",
      "Action": [
        "account:GetAccountInformation",
        "account:ListRegions",
        "account:PutContactInformation",
        "account:PutAlternateContact",
        "account>DeleteAlternateContact",
        "account:EnableRegion",
        "account:DisableRegion"
      ],
      "Resource": "*"
    }
  ]
}
```

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Pengelolaan Akun

Untuk diskusi lengkap tentang Akun AWS dan pengguna IAM, lihat [Apa itu IAM?](#) di Panduan Pengguna IAM.

Untuk petunjuk tentang cara memperbarui kebijakan yang dikelola pelanggan, lihat [Mengedit kebijakan IAM](#) di Panduan Pengguna IAM.

AWS Kebijakan tindakan Manajemen Akun

Tabel ini merangkum izin yang memberikan akses ke pengaturan akun Anda. Untuk contoh kebijakan yang menggunakan izin ini, lihat [Identity-based contoh kebijakan untuk AWS Pengelolaan Akun](#).

Note

Untuk memberikan akses tulis kepada pengguna IAM ke setelan [akun tertentu di halaman Akun](#) Konsol Manajemen AWS, Anda harus mengizinkan `GetAccountInformation` izin, selain izin (atau izin) yang ingin Anda gunakan untuk mengubah setelan itu.

Nama izin	Tingkat akses	Deskripsi
<code>account:ListRegions</code>	Daftar	Memberikan izin untuk membuat daftar Wilayah yang tersedia.
<code>account:GetAccountInformation</code>	Baca	Memberikan izin untuk mengambil informasi akun untuk akun.
<code>account:GetAlternateContact</code>	Baca	Memberikan izin untuk mengambil kontak alternatif untuk akun.
<code>account:GetContactInformation</code>	Baca	Memberikan izin untuk mengambil informasi kontak utama untuk akun.
<code>account:GetPrimaryEmail</code>	Baca	Memberikan izin untuk mengambil alamat email utama akun.

Nama izin	Tingkat akses	Deskripsi
<code>account:GetRegionOptStatus</code>	Baca	Memberikan izin untuk mendapatkan status keikutsertaan suatu Wilayah.
<code>account:AcceptPrimaryEmailUpdate</code>	Tulis	Memberikan izin untuk menerima pembaruan alamat email utama akun anggota dalam suatu AWS organisasi.
<code>account:CloseAccount</code>	Tulis	Memberikan izin untuk menutup akun. <div data-bbox="1068 751 1507 1066" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Ini adalah izin untuk konsol saja. Tidak ada akses API yang tersedia untuk izin ini.</p> </div>
<code>account>DeleteAlternateContact</code>	Tulis	Memberikan izin untuk menghapus kontak alternatif untuk akun.
<code>account:DisableRegion</code>	Tulis	Memberikan izin untuk menonaktifkan penggunaan Wilayah.
<code>account:EnableRegion</code>	Tulis	Memberikan izin untuk mengaktifkan penggunaan Wilayah.
<code>account:PutAccountName</code>	Tulis	Memberikan izin untuk memperbarui nama akun.

Nama izin	Tingkat akses	Deskripsi
<code>account:PutAlternativeContact</code>	Tulis	Memberikan izin untuk memodifikasi kontak alternatif untuk akun.
<code>account:PutContactInformation</code>	Tulis	Memberikan izin untuk memperbarui informasi kontak utama untuk akun.
<code>account:StartPrimaryEmailUpdate</code>	Tulis	Memberikan izin untuk memulai pembaruan alamat email utama akun anggota dalam suatu AWS organisasi.

Pemecahan masalah AWS Identitas dan akses Manajemen Akun

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Manajemen Akun dan IAM.


Topik

- [Saya tidak berwenang untuk melakukan tindakan di halaman Akun](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses detail akun saya](#)

Saya tidak berwenang untuk melakukan tindakan di halaman Akun

Jika Konsol Manajemen AWS memberitahu Anda bahwa Anda tidak berwenang untuk melakukan suatu tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk melihat detail tentangnya Akun AWS di halaman Akun Konsol Manajemen AWS tetapi tidak memiliki `account:GetAccountInformation` izin.



You Need Permissions

You don't have permission to access billing information for this account. Contact your AWS administrator if you need help. If you are an AWS administrator, you can provide permissions for your users or groups by making sure that (1) [this account allows IAM and federated users to access billing information](#) and (2) [you have the required IAM permissions](#).

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *my-example-widget* menggunakan tindakan `account:GetWidget`.

Saya tidak berwenang untuk melakukan `iam:PassRole`

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Manajemen Akun.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan dalam Manajemen Akun. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses detail akun saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Manajemen Akun mendukung fitur ini, lihat [Bagaimana AWS Manajemen Akun bekerja dengan IAM](#).
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

AWS kebijakan terkelola untuk Manajemen AWS Akun

AWS Manajemen Akun saat ini menyediakan dua kebijakan AWS terkelola yang tersedia untuk Anda gunakan:

- [AWS kebijakan terkelola: AWSAccount ManagementReadOnlyAccess](#)
- [AWS kebijakan terkelola: AWSAccount ManagementFullAccess](#)
- [Pembaruan Manajemen Akun ke kebijakan AWS terkelola](#)

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS

kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

AWS kebijakan terkelola: AWSAccount ManagementReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSAccountManagementReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini menyediakan izin hanya-baca untuk hanya melihat hal-hal berikut:

- Metadata tentang Anda Akun AWS
- Wilayah AWS Yang diaktifkan atau dinonaktifkan untuk Akun AWS (Anda dapat melihat status Wilayah di akun Anda hanya dengan menggunakan AWS konsol)

Hal ini dilakukan dengan memberikan izin untuk menjalankan salah satu `Get*` atau `List*` operasi. Itu tidak memberikan kemampuan untuk mengubah metadata akun atau mengaktifkan atau menonaktifkan Wilayah AWS akun.

Detail izin

Kebijakan ini mencakup izin berikut.

- `account`— Memungkinkan kepala sekolah untuk mengambil informasi metadata tentang. Akun AWS Hal ini juga memungkinkan prinsipal untuk daftar Wilayah AWS yang diaktifkan untuk akun di Konsol Manajemen AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "account:Get*",
        "account:List*"
      ],
    },
  ],
}
```

```
        "Resource": "*"
    }
  ]
}
```

AWS kebijakan terkelola: AWSAccount ManagementFullAccess

Anda dapat melampirkan kebijakan `AWSAccountManagementFullAccess` ke identitas IAM Anda.

Kebijakan ini menyediakan akses administratif penuh untuk melihat atau memodifikasi hal-hal berikut:

- Metadata tentang Anda Akun AWS
- Wilayah AWS Yang diaktifkan atau dinonaktifkan untuk Akun AWS (Anda dapat melihat status atau mengaktifkan atau menonaktifkan Wilayah untuk akun Anda hanya dengan menggunakan AWS konsol)

Ini dilakukan dengan memberikan izin untuk menjalankan account operasi apa pun.

Detail izin

Kebijakan ini mencakup izin berikut.

- `account`— Memungkinkan kepala sekolah untuk melihat atau memodifikasi informasi metadata tentang Akun AWS Hal ini juga memungkinkan prinsipal untuk daftar Wilayah AWS yang diaktifkan untuk akun dan mengaktifkan atau menonaktifkannya di Konsol Manajemen AWS

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "account:*",
      "Resource": "*"
    }
  ]
}
```

Pembaruan Manajemen Akun ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Manajemen Akun sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Manajemen Akun.

Ubah	Deskripsi	Date
AWS Manajemen Akun diluncurkan dengan kebijakan AWS terkelola baru dan mulai melacak perubahan	<p>Manajemen Akun awalnya diluncurkan dengan kebijakan AWS terkelola berikut:</p> <ul style="list-style-type: none"> • AWSAccountManagementReadOnlyAccess • AWSAccountManagementFullAccess 	30 September 2021

Validasi kepatuhan untuk Manajemen AWS Akun

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS layanan yang dapat dijalankan di Anda Akun AWS sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.


Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS dalam lingkup berdasarkan program kepatuhan Layanan AWS](#) . Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#) .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [AWS Artifact Mengunduh](#) Mengunduh Laporan AWS Artifact di Panduan AWS Artifact Pengguna.

Tanggung jawab kepatuhan Anda saat menggunakan layanan Akun AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan](#) penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.

- [Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services](#) — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

 Note

Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat [Referensi Layanan yang Memenuhi Syarat HIPAA](#).

- [AWS Sumber Daya AWS](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [Mengevaluasi Sumber Daya dengan Aturan](#) dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub CSPM](#)— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.
- [AWS Audit Manager](#)Ini Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan dalam Manajemen Akun AWS

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Keamanan infrastruktur di AWS Account Management

Sebagai layanan terkelola, AWS layanan Akun AWS yang berjalan di Anda dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan](#).

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses pengaturan akun melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan principal IAM. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Pantau Anda Akun AWS

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja Manajemen AWS Akun dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk menonton Manajemen Akun, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- AWS CloudTrail menangkap (log) panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan menulis file log ke bucket Amazon Simple Storage Service (Amazon S3) yang Anda tentukan. Ini memungkinkan Anda mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, silakan lihat [Panduan Pengguna AWS CloudTrail](#).
- Amazon EventBridge menambahkan otomatisasi tambahan ke AWS layanan Anda dengan merespons secara otomatis peristiwa sistem, seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Acara dari AWS layanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihat [Panduan EventBridge Pengguna Amazon](#).

Logging AWS Account Management API menggunakan AWS CloudTrail

Manajemen AWS APIs Akun terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan yang memanggil operasi Manajemen Akun. CloudTrail menangkap semua panggilan Account Management API sebagai event. Panggilan yang diambil mencakup semua panggilan ke operasi Manajemen Akun. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk operasi Manajemen Akun. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang disebut operasi Manajemen Akun, alamat IP yang digunakan untuk membuat permintaan, siapa yang membuat permintaan dan kapan, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

Informasi Manajemen Akun di CloudTrail

CloudTrail dihidupkan di Anda Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi dengan operasi Manajemen Akun, CloudTrail mencatat aktivitas tersebut dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat [Melihat Acara dengan Riwayat CloudTrail Acara](#).

Untuk catatan peristiwa yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk operasi Manajemen Akun, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di Konsol Manajemen AWS, jejak berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- [Gambaran umum untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa Wilayah](#)
- [Menerima file CloudTrail log dari beberapa akun](#)

AWS CloudTrail mencatat semua operasi API Manajemen Akun yang ditemukan di bagian [Referensi API](#) dari panduan ini. Misalnya, panggilan ke `CreateAccount`, `DeleteAlternateContact`, dan `PutAlternateContact` operasi menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan pengguna root atau kredensial pengguna AWS Identity and Access Management (IAM)
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk peran IAM atau pengguna federasi
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Memahami entri log Manajemen Akun

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber mana pun dan mencakup informasi tentang operasi yang diminta, tanggal dan waktu operasi, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh 1: Contoh berikut menunjukkan entri CloudTrail log untuk panggilan ke `GetAlternateContact` operasi untuk mengambil kontak OPERATIONS alternatif saat ini untuk akun. Nilai yang dikembalikan oleh operasi tidak disertakan dalam informasi yang dicatat.

Example Contoh 1

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T19:25:53Z"
      }
    }
  },
  "eventTime": "2021-04-30T19:26:15Z",
  "eventSource": "account.amazonaws.com",
  "eventName": "GetAlternateContact",
  "awsRegion": "us-east-1",
```

```

"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "alternateContactType": "SECURITY"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-111111111111",
"eventID": "1a2b3c4d-5e6f-1234-abcd-222222222222",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}

```

Contoh 2: Contoh berikut menunjukkan entri CloudTrail log untuk panggilan ke `PutAlternateContact` operasi untuk menambahkan kontak BILLING alternatif baru ke akun.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-04-30T18:33:00Z"
      }
    }
  },
  "eventTime": "2021-04-30T18:33:08Z",
  "eventSource": "account.amazonaws.com",

```

```

"eventName": "PutAlternateContact",
"awsRegion": "us-east-1",
"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "name": "*Alejandro Rosalez*",
  "emailAddress": "alrosalez@example.com",
  "title": "CFO",
  "alternateContactType": "BILLING"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-333333333333",
"eventID": "1a2b3c4d-5e6f-1234-abcd-444444444444",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}

```

Contoh 3: Contoh berikut menunjukkan entri CloudTrail log untuk panggilan ke `DeleteAlternateContact` operasi untuk menghapus kontak OPERATIONS alternatif saat ini.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI234567890EXAMPLE:AccountAPITests",
    "arn": "arn:aws:sts::123456789012:assumed-role/ServiceTestRole/AccountAPITests",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI234567890EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/ServiceTestRole",
        "accountId": "123456789012",
        "userName": "ServiceTestRole"
      }
    },
    "webIdFederationData": {},
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2021-04-30T18:33:00Z"
    }
  }
}

```

```
    }
  }
},
"eventTime": "2021-04-30T18:33:16Z",
"eventSource": "account.amazonaws.com",
"eventName": "DeleteAlternateContact",
"awsRegion": "us-east-1",
"sourceIPAddress": "10.24.34.250",
"userAgent": "Mozilla/5.0",
"requestParameters": {
  "alternateContactType": "OPERATIONS"
},
"responseElements": null,
"requestID": "1a2b3c4d-5e6f-1234-abcd-555555555555",
"eventID": "1a2b3c4d-5e6f-1234-abcd-666666666666",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012"
}
```

Memantau acara Manajemen Akun dengan EventBridge

Amazon EventBridge, sebelumnya disebut CloudWatch Events, membantu Anda memantau peristiwa yang khusus untuk Manajemen Akun dan memulai tindakan target yang menggunakan lainnya.

Layanan AWS Acara dari Layanan AWS dikirim ke EventBridge dalam waktu dekat.

Dengan menggunakan EventBridge, Anda dapat membuat aturan yang cocok dengan peristiwa yang masuk dan merutekannya ke target untuk diproses.

Untuk informasi selengkapnya, lihat [Memulai Amazon EventBridge](#) di Panduan EventBridge Pengguna Amazon.

Acara Manajemen Akun

Contoh berikut menunjukkan peristiwa untuk Manajemen Akun. Acara diproduksi atas dasar upaya terbaik.

Hanya peristiwa yang khusus untuk mengaktifkan dan menonaktifkan Regions dan panggilan API via yang saat ini CloudTrail tersedia untuk Manajemen Akun.

Tipe peristiwa

- [Acara untuk mengaktifkan dan menonaktifkan Wilayah](#)

Acara untuk mengaktifkan dan menonaktifkan Wilayah

Saat Anda mengaktifkan atau menonaktifkan Wilayah di akun, baik dari Konsol maupun dari API, tugas asinkron akan dimulai. Permintaan awal akan dicatat sebagai CloudTrail peristiwa di akun target. Selain itu, sebuah EventBridge acara akan dikirim ke akun panggilan ketika proses aktifkan atau nonaktifkan telah dimulai, dan sekali lagi setelah proses tersebut selesai.

Contoh peristiwa berikut menunjukkan bagaimana permintaan akan dikirim yang menunjukkan bahwa 2020-09-30 di ap-east-1 Wilayah adalah ENABLED untuk akun123456789012.

```
{
  "version":"0",
  "id":"11112222-3333-4444-5555-666677778888",
  "detail-type":"Region Opt-In Status Change",
  "source":"aws.account",
  "account":"123456789012",
  "time":"2020-09-30T06:51:08Z",
  "region":"us-east-1",
  "resources":[
    "arn:aws:account::123456789012:account"
  ],
  "detail":{
    "accountId":"123456789012",
    "regionName":"ap-east-1",
    "status":"ENABLED"
  }
}
```

Ada empat kemungkinan status yang cocok dengan status yang dikembalikan oleh API `GetRegionOptStatus` dan `ListRegions`:

- **ENABLED**— Wilayah telah berhasil diaktifkan untuk yang `accountId` ditunjukkan
- **ENABLING**— Wilayah sedang dalam proses diaktifkan untuk yang `accountId` ditunjukkan
- **DISABLED**- Wilayah telah berhasil dinonaktifkan untuk yang `accountId` ditunjukkan
- **DISABLING**— Wilayah sedang dalam proses dinonaktifkan untuk yang `accountId` ditunjukkan

Contoh pola peristiwa berikut membuat aturan yang menangkap semua peristiwa Region.

```
{
  "source": [
    "aws.account"
  ],
  "detail-type": [
    "Region Opt-In Status Change"
  ]
}
```

Contoh pola peristiwa berikut membuat aturan yang hanya menangkap peristiwa ENABLED dan DISABLED Wilayah.

```
{
  "source": [
    "aws.account"
  ],
  "detail-type": [
    "Region Opt-In Status Change"
  ],
  "detail": {
    "status": [
      "DISABLED",
      "ENABLED"
    ]
  }
}
```

Memecahkan masalah Anda Akun AWS

Gunakan informasi dalam topik berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah Anda Akun AWS. Untuk bantuan dengan pengguna root, lihat [Memecahkan masalah dengan pengguna root di Panduan Pengguna IAM](#). Untuk bantuan terkait proses login, lihat [Memecahkan masalah Akun AWS login](#) di Panduan Pengguna Masuk.AWS

Topik-topik penyelesaian masalah

- [Memecahkan masalah dengan Akun AWS pembuatan](#)
- [Memecahkan masalah dengan penutupan Akun AWS](#)
- [Memecahkan masalah lain dengan Akun AWS](#)

Memecahkan masalah dengan Akun AWS pembuatan

Gunakan tautan referensi dalam tabel berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah dengan membuat yang baru Akun AWS.

Isu	Tautan referensi	Sumber
Saya tidak tahu cara mendaftar atau membuat akun	Memulai dengan Akun AWS	Panduan ini
Apa yang harus saya lakukan jika saya tidak menerima panggilan AWS untuk memverifikasi akun baru saya atau PIN yang saya masukkan tidak berfungsi?	https://repost.aws/knowledge-center/phone-verify-no-call	AWS re:Post
Bagaimana cara mengatasi kesalahan “jumlah maksimum upaya yang gagal” ketika saya mencoba memverifikasi Akun AWS melalui telepon?	https://repost.aws/knowledge-center/maximum-failed-attempts	AWS re:Post

Isu	Tautan referensi	Sumber
Sudah lebih dari 24 jam dan akun saya tidak diaktifkan	https://repost.aws/knowledge-center/create-and-activate-aws-account	AWS re:Post
Saya tidak dapat masuk ke akun baru saya setelah dibuat	https://docs.aws.amazon.com/signin/latest/userguide/troubleshooting-sign-in-issues.html	AWS Sign-In Panduan Pengguna

Untuk bantuan tambahan, kami sarankan Anda [AWS re:Post](#) mencari konten yang terkait dengan masalah spesifik Anda. Jika Anda masih membutuhkan bantuan, hubungi [AWS Dukungan](#).

Memecahkan masalah dengan penutupan Akun AWS

Gunakan informasi di bawah ini untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang ditemukan selama proses penutupan akun. Untuk informasi umum tentang proses penutupan akun, lihat [Tutup sebuah Akun AWS](#).

Topik

- [Saya tidak tahu cara menghapus atau membatalkan akun saya](#)
- [Saya tidak melihat tombol Tutup akun di halaman Akun](#)
- [Saya menutup akun saya tetapi masih belum menerima konfirmasi email](#)
- [Saya menerima kesalahan ConstraintViolationException "" saat mencoba menutup akun saya](#)
- [Saya menerima kesalahan "CLOSE_ACCOUNT_QUOTA_EXCEEDED" saat mencoba menutup akun anggota](#)
- [Apakah saya perlu menghapus AWS organisasi saya sebelum menutup akun manajemen?](#)

Saya tidak tahu cara menghapus atau membatalkan akun saya

Untuk menutup akun Anda, ikuti instruksi di [Tutup sebuah Akun AWS](#).

Saya tidak melihat tombol Tutup akun di halaman Akun

Jika Anda tidak masuk sebagai pengguna root, Anda tidak akan melihat tombol Tutup akun yang ditampilkan di halaman Akun. Anda harus [Masuk ke Konsol Manajemen AWS sebagai pengguna](#)

[root](#) untuk menutup akun Anda. Jika Anda tidak dapat masuk, lihat [Memecahkan masalah dengan pengguna root](#).

Saya menutup akun saya tetapi masih belum menerima konfirmasi email

Email konfirmasi ini hanya dikirim ke alamat email pengguna root alamat email untuk Akun AWS. Jika Anda tidak menerima email ini dalam beberapa jam, Anda dapat [Masuk ke Konsol Manajemen AWS sebagai pengguna root](#) untuk memeriksa apakah akun Anda ditutup. Jika akun Anda berhasil ditutup, Anda akan melihat pesan yang ditampilkan yang menunjukkan akun Anda ditutup. Jika akun yang Anda tutup adalah akun anggota, Anda dapat memverifikasi penutupan yang berhasil dengan memeriksa apakah akun yang ditutup diberi label seperti CLOSED di AWS Organizations konsol. Untuk informasi selengkapnya, lihat [Menutup akun anggota di organisasi Anda](#) di Panduan AWS Organizations Pengguna.

Jika Anda mencoba menutup akun manajemen dan tidak menerima konfirmasi email tentang penutupan akun, organisasi Anda kemungkinan besar memiliki akun anggota aktif. Anda hanya dapat menutup akun manajemen jika organisasi Anda tidak memiliki akun anggota aktif. Untuk memverifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda, buka AWS Organizations konsol, dan pastikan semua akun anggota ditampilkan di Closed sebelah nama akun mereka. Setelah itu, Anda dapat menutup akun manajemen.

Saya menerima kesalahan ConstraintViolationException "" saat mencoba menutup akun saya

Anda mencoba menutup akun manajemen menggunakan AWS Organizations konsol, yang tidak mungkin. Untuk menutup akun manajemen, Anda harus [Masuk ke Konsol Manajemen AWS sebagai pengguna root](#) untuk akun manajemen dan menutupnya dari halaman Akun. Untuk informasi selengkapnya, lihat [Menutup akun manajemen di organisasi Anda](#) di Panduan AWS Organizations Pengguna.

Saya menerima kesalahan "CLOSE_ACCOUNT_QUOTA_EXCEEDED" saat mencoba menutup akun anggota

Anda hanya dapat menutup 10% akun anggota dalam periode 30 hari bergulir. Kuota ini tidak terikat oleh bulan kalender, tetapi dimulai ketika Anda menutup akun. Dalam 30 hari sejak penutupan akun awal, Anda tidak dapat melebihi batas penutupan akun 10%. Penutupan akun minimum adalah 10 dan penutupan akun maksimum adalah 1000, bahkan jika 10% akun melebihi 1000. Untuk

informasi selengkapnya tentang kuota Organizations, lihat [Kuota untuk AWS Organizations](#) di AWS Organizations Panduan Pengguna.

Apakah saya perlu menghapus AWS organisasi saya sebelum menutup akun manajemen?

Tidak, Anda tidak perlu menghapus AWS organisasi Anda sebelum menutup akun manajemen. Namun, Anda hanya dapat menutup akun manajemen jika organisasi Anda tidak memiliki akun anggota aktif. Untuk memverifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda, buka AWS Organizations konsol, dan pastikan semua akun anggota ditampilkan di Closed sebelah nama akun mereka. Setelah itu, Anda dapat menutup akun manajemen.

Memecahkan masalah lain dengan Akun AWS

Gunakan informasi di sini untuk membantu Anda memecahkan masalah yang terkait dengan Anda. Akun AWS

Masalah

- [Saya perlu mengganti kartu kredit untuk saya Akun AWS](#)
- [Saya perlu melaporkan penipuan Akun AWS aktivitas](#)
- [Aku harus menutup Akun AWS](#)

Saya perlu mengganti kartu kredit untuk saya Akun AWS

Untuk mengganti kartu kredit Anda Akun AWS, Anda harus dapat masuk. AWS memiliki perlindungan di tempat yang mengharuskan Anda untuk membuktikan bahwa Anda adalah pemilik akun. Untuk petunjuk, lihat [Mengelola metode pembayaran kartu kredit Anda](#) di Panduan AWS Billing Pengguna.

Saya perlu melaporkan penipuan Akun AWS aktivitas

Jika Anda mencurigai aktivitas penipuan menggunakan Anda Akun AWS dan ingin membuat laporan, lihat [Bagaimana cara melaporkan penyalahgunaan sumber daya. AWS](#)

Jika Anda mengalami masalah dengan pembelian yang dilakukan Amazon.com, lihat [Layanan Pelanggan Amazon](#).

Aku harus menutup Akun AWS

Untuk membantu memecahkan masalah dengan menutup masalah Anda Akun AWS, lihat. [Tutup sebuah Akun AWS](#)

Tutup sebuah Akun AWS

Jika Anda tidak lagi membutuhkannya Akun AWS, Anda dapat menutupnya kapan saja dengan mengikuti instruksi di bagian ini. Setelah Anda menutupnya, Anda dapat membukanya kembali dalam waktu 90 hari sejak Anda menutup akun. [Jangka waktu antara hari Anda menutup akun dan ketika menutup akun AWS secara permanen disebut sebagai periode pasca-penutupan.](#)

Apa yang perlu Anda ketahui sebelum menutup akun Anda

Sebelum menutup Anda Akun AWS, Anda harus mempertimbangkan hal berikut:

- Menutup akun Anda akan berfungsi sebagai pemberitahuan penghentian Perjanjian AWS Pelanggan untuk akun ini.
- Anda tidak perlu menghapus sumber daya Akun AWS sebelum menutupnya. Namun, kami sarankan Anda mencadangkan sumber daya atau data apa pun yang ingin Anda simpan. Untuk petunjuk tentang cara membuat cadangan sumber daya tertentu, lihat [AWS dokumentasi](#) yang sesuai untuk layanan tersebut.
- Anda dapat membuka kembali akun Anda selama periode [pasca-penutupan](#). Biaya untuk layanan yang tersisa di akun Anda akan dimulai ulang jika Anda membukanya kembali. [Anda juga tetap bertanggung jawab atas faktur yang belum dibayar dan Instans Cadangan dan Savings Plans yang belum dibayar.](#)
- Anda tetap bertanggung jawab atas semua biaya dan biaya yang belum dibayar untuk layanan yang dikonsumsi sebelum penutupan akun. Anda akan menerima AWS tagihan pada bulan berikutnya setelah menutup akun Anda. Misalnya, jika Anda menutup akun Anda pada 15 Januari, Anda akan menerima tagihan pada awal Februari untuk penggunaan yang terjadi dari 1 Januari hingga 15 Januari. Anda akan terus menerima faktur untuk [Instans Cadangan dan Savings Plans](#) setelah menutup akun Anda hingga habis masa berlakunya.
- Anda tidak akan lagi dapat mengakses AWS layanan yang sebelumnya tersedia di akun Anda. Namun, Anda dapat masuk dan mengakses penutupan Akun AWS selama [periode pasca-penutupan](#) hanya untuk melihat informasi penagihan sebelumnya, mengakses pengaturan akun, atau kontak. [AWS Dukungan](#)
- Anda tidak dapat menggunakan alamat email yang sama yang terdaftar Akun AWS pada Anda pada saat penutupan sebagai email utama orang lain Akun AWS. Jika Anda ingin menggunakan alamat email yang sama untuk yang berbeda Akun AWS, kami sarankan untuk memperbaruinya sebelum penutupan. Untuk informasi selengkapnya, lihat [Perbarui alamat email pengguna root.](#)

- Jika Anda telah [mengaktifkan otentikasi multi-faktor \(MFA\)](#) pada pengguna Akun AWS root Anda, atau mengonfigurasi [perangkat MFA pada pengguna IAM, MFA tidak akan dihapus](#) secara otomatis saat Anda menutup akun. Jika Anda memilih untuk membiarkan MFA dihidupkan selama [periode 90 hari pasca-penutupan](#), jaga agar perangkat MFA tetap aktif hingga periode pasca-penutupan berakhir jika Anda perlu mengakses akun selama waktu itu. Catatan, perangkat token TOTP perangkat keras tidak dapat dikaitkan dengan pengguna lain setelah penutupan permanen akun Anda. Jika Anda ingin menggunakan token TOTP perangkat keras dengan pengguna lain nanti, Anda memiliki opsi untuk [menonaktifkan perangkat MFA perangkat keras](#) sebelum menutup akun. Perangkat MFA untuk [pengguna IAM](#) harus dihapus oleh administrator akun.

Pertimbangan tambahan untuk akun anggota

- Saat Anda menutup akun anggota, akun tersebut tidak akan dihapus dari organisasi sampai setelah [periode pasca-penutupan](#). Selama periode pasca-penutupan, akun anggota tertutup masih diperhitungkan dalam kuota akun Anda di organisasi. Untuk menghindari jumlah akun terhadap kuota, lihat [Menghapus akun anggota dari organisasi Anda](#) sebelum menutupnya.
- Anda hanya dapat menutup 20% atau 250 akun anggota hingga maksimum 1.000 dalam periode 30 hari bergulir, mana yang lebih tinggi. Kuota ini tidak terikat oleh bulan kalender, tetapi dimulai ketika Anda menutup akun. Untuk informasi selengkapnya tentang kuota Organizations, lihat [Kuota](#) untuk AWS Organizations
- Jika Anda menggunakan AWS Control Tower, Anda harus membatalkan kelola akun anggota sebelum mencoba menutup akun. Lihat [Membatalkan kelola akun anggota](#) di Panduan Pengguna AWS Control Tower.

Pertimbangan khusus layanan

- AWS Marketplace langganan tidak dibatalkan secara otomatis pada penutupan akun. Jika Anda memiliki langganan, pertama-tama [hentikan semua instance perangkat lunak Anda](#) di langganan. Kemudian, buka halaman [Kelola langganan](#) AWS Marketplace konsol dan batalkan langganan Anda.
- Setelah akun ditutup, AWS akan mengirim email harian hingga lima hari sebelum kami menangguhkan domain. Setelah domain ditangguhkan, dan tergantung pada registrar domain, kami akan menghapus domain dalam waktu 30 hari atau melepaskan domain ke pendaftarnya. Untuk informasi selengkapnya, lihat [Akun AWS Milik saya ditutup atau ditutup secara permanen, dan domain saya terdaftar di Route 53](#).

- AWS CloudTrail adalah layanan keamanan dasar. Ini berarti bahwa jejak yang dibuat oleh pengguna dapat terus ada dan mengirimkan peristiwa bahkan setelah Akun AWS ditutup, kecuali pengguna secara eksplisit menghapus jejak di dalamnya sebelum menutupnya. Akun AWS Untuk informasi selengkapnya tentang cara meminta penghapusan jejak Akun AWS setelah ditutup, lihat [Akun AWS penutupan dan jejak di Panduan Pengguna](#). CloudTrail

Cara menutup akun Anda

Anda dapat menutup Akun AWS menggunakan prosedur berikut. Perhatikan, bahwa ada panduan berbeda yang disediakan di setiap tab tergantung pada jenis akun [mandiri, anggota, manajemen, dan AWS GovCloud (US)] yang ingin Anda tutup.

Jika Anda mengalami masalah apa pun selama proses penutupan akun, lihat [Memecahkan masalah dengan penutupan Akun AWS](#).

Standalone account

Akun mandiri adalah akun yang dikelola secara individual yang bukan merupakan bagian dari AWS Organizations

Untuk menutup akun mandiri dari halaman Akun

1. [Masuk ke Konsol Manajemen AWS sebagai pengguna root](#) di Akun AWS yang ingin Anda tutup. Anda tidak dapat menutup akun saat masuk sebagai pengguna atau peran IAM.
2. Pada bilah navigasi di sudut kanan atas, pilih nama atau nomor akun Anda, lalu pilih Akun.
3. Pada [halaman Akun](#), pilih tombol Tutup akun.
4. Ketik ID akun Anda (ditampilkan di bagian atas kotak dialog penutupan) untuk mengonfirmasi bahwa Anda telah membaca dan memahami proses penutupan akun.
5. Pilih tombol Tutup akun untuk memulai proses penutupan akun.
6. Dalam beberapa menit, Anda akan menerima konfirmasi email bahwa akun Anda telah ditutup.

Note

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

Member account

Akun anggota Akun AWS adalah bagian dari AWS Organizations.

Untuk menutup akun anggota dari AWS Organizations konsol

1. Masuk ke [konsol AWS Organizations](#) tersebut.
2. Pada Akun AWS halaman, temukan dan pilih nama akun anggota yang ingin Anda tutup. Anda dapat menavigasi hierarki OU, atau melihat daftar datar akun tanpa struktur OU.
3. Pilih Tutup di sebelah nama akun di bagian atas halaman. Opsi ini hanya tersedia ketika AWS organisasi berada dalam mode [Semua fitur](#).

Note

Jika organisasi Anda menggunakan mode [penagihan Konsolidasi](#), Anda tidak akan dapat melihat tombol Tutup di konsol. Untuk menutup akun dalam mode penagihan gabungan, masuk ke akun yang ingin Anda tutup sebagai pengguna root. Pada halaman Akun, pilih tombol Tutup akun, masukkan ID akun Anda, lalu pilih tombol Tutup akun.

4. Baca dan pastikan Anda memahami panduan penutupan akun.
5. Masukkan ID akun anggota, lalu pilih Tutup akun untuk memulai proses penutupan akun.

Note

Setiap akun anggota yang Anda tutup akan menampilkan CLOSED label di sebelah nama akunnya di AWS Organizations konsol hingga 90 hari setelah tanggal penutupan asli. Setelah 90 hari, akun anggota tidak akan lagi ditampilkan di AWS Organizations konsol.

Untuk menutup akun anggota dari halaman Akun

Secara opsional, Anda dapat menutup akun AWS anggota langsung dari [halaman Akun](#) di Konsol Manajemen AWS Untuk panduan langkah demi langkah, ikuti petunjuk di tab Akun mandiri.

Untuk menutup akun anggota menggunakan AWS CLI dan SDK

Untuk petunjuk tentang cara menutup akun anggota menggunakan AWS CLI dan SDK, lihat [Menutup akun anggota di organisasi Anda](#) di Panduan AWS Organizations Pengguna.

Management account

Akun manajemen adalah akun Akun AWS yang bertindak sebagai akun induk atau root untuk AWS Organizations.

Note

Anda tidak dapat menutup akun manajemen langsung dari AWS Organizations konsol.

Untuk menutup akun manajemen dari halaman Akun

1. [Masuk ke Konsol Manajemen AWS sebagai pengguna root](#) untuk akun manajemen yang ingin Anda tutup. Anda tidak dapat menutup akun saat masuk sebagai pengguna atau peran IAM.
2. Verifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda. Untuk melakukan ini, buka [AWS Organizations konsol](#), dan pastikan semua akun anggota ditampilkan di **C**losed sebelah nama akun mereka. Jika Anda memiliki akun anggota yang masih aktif, Anda harus mengikuti panduan penutupan akun yang disediakan di tab Akun Anggota sebelum Anda dapat melanjutkan ke langkah berikutnya.
3. Pada bilah navigasi di sudut kanan atas, pilih nama atau nomor akun Anda, lalu pilih Akun.
4. Pada [halaman Akun](#), pilih tombol Tutup akun.
5. Ketik ID akun Anda (ditampilkan di bagian atas kotak dialog penutupan) untuk mengonfirmasi bahwa Anda telah membaca dan memahami proses penutupan akun.
6. Pilih tombol Tutup akun untuk memulai proses penutupan akun.
7. Dalam beberapa menit, Anda akan menerima konfirmasi email bahwa akun Anda telah ditutup.

Note

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan Konsol Manajemen AWS.

AWS GovCloud (US) account

AWS GovCloud (US) Akun selalu ditautkan ke satu standar Akun AWS untuk tujuan penagihan dan pembayaran.

Untuk menutup AWS GovCloud (US) akun

Jika Anda memiliki akun Akun AWS yang ditautkan ke AWS GovCloud (US) akun, Anda harus menutup akun standar sebelum menutup AWS GovCloud (US) akun. Untuk detail selengkapnya, termasuk cara mencadangkan data dan menghindari AWS GovCloud (US) tagihan yang tidak diinginkan, lihat [Menutup AWS GovCloud \(US\) akun](#) di AWS GovCloud (US) Panduan Pengguna.

Apa yang diharapkan setelah Anda menutup akun Anda

Segera setelah Anda menutup akun Anda, hal berikut akan terjadi:

- Anda akan menerima email yang mengonfirmasi penutupan akun ke alamat email pengguna root. Jika Anda tidak menerima email ini dalam beberapa jam, lihat [Memecahkan masalah dengan penutupan Akun AWS](#).
- Setiap akun anggota yang Anda tutup akan menampilkan CLOSED label di sebelah nama akunnya di AWS Organizations konsol hingga 90 hari setelah tanggal penutupan asli. Setelah 90 hari, akun anggota tidak akan lagi ditampilkan di AWS Organizations konsol.
- Jika Anda telah memberikan izin untuk mengakses layanan di akun Anda Akun AWS ke akun lain, permintaan akses apa pun yang dibuat dari akun tersebut akan gagal setelah penutupan akun. Jika Anda membuka kembali Akun AWS, orang lain Akun AWS dapat kembali mengakses AWS layanan dan sumber daya akun Anda jika Anda memberikan izin yang diperlukan kepada mereka.

Penutupan akun mungkin tidak segera terjadi di semua Wilayah dan layanan dan dapat memakan waktu beberapa jam untuk menyelesaikannya.

Post-closure periode

Periode pasca-penutupan mengacu pada lamanya waktu antara hari Anda menutup akun Anda dan ketika menutup akun Anda AWS secara permanen. Akun AWS Periode pasca-penutupan adalah 90 hari. Selama periode pasca-penutupan, Anda dapat mengakses konten dan AWS layanan Anda hanya dengan membuka kembali akun Anda. Setelah periode pasca-penutupan, tutup AWS secara permanen Akun AWS, dan Anda tidak dapat lagi membukanya kembali. AWS juga akan menghapus

konten dan sumber daya di akun Anda (kecuali untuk CloudTrail jejak). Setelah akun ditutup secara permanen, [Akun AWS ID-nya](#) tidak akan pernah dapat digunakan kembali.

Membuka kembali Anda Akun AWS

Akun Anda akan ditutup secara permanen dalam 90 hari, setelah itu Anda tidak akan dapat membuka kembali akun Anda dan AWS akan menghapus konten yang tersisa di akun Anda. Untuk membuka kembali akun Anda sebelum ditutup secara permanen, (1) Anda harus menghubungi [AWS Dukungan](#) sesegera mungkin, dan (2) kami harus menerima pembayaran penuh dari saldo terutang, termasuk memberikan informasi yang diperlukan sebagaimana ditentukan pada faktur, dalam waktu 30 hari sejak tanggal penutupan akun.

Note

Biaya untuk layanan yang tersisa di akun Anda akan dimulai ulang jika Anda membukanya kembali.

Referensi API

Operasi API di namespace Account Management (`account`) memungkinkan Anda untuk memodifikasi. Akun AWS

Masing-masing Akun AWS mendukung metadata dengan informasi tentang akun, termasuk informasi tentang hingga tiga kontak alternatif yang terkait dengan akun. Ini adalah tambahan untuk alamat email yang terkait dengan [pengguna root](#) akun. Anda hanya dapat menentukan satu dari masing-masing jenis kontak berikut yang terkait dengan akun.

- Kontak penagihan
- Kontak operasi
- Kontak keamanan

Secara default, operasi API yang dibahas dalam panduan ini berlaku langsung ke akun yang memanggil operasi. [Identitas](#) dalam akun yang memanggil operasi biasanya merupakan peran IAM atau pengguna IAM dan harus memiliki izin yang diterapkan oleh kebijakan IAM untuk memanggil operasi API. Atau, Anda dapat memanggil operasi API ini dari identitas di akun AWS Organizations manajemen dan menentukan nomor ID akun untuk setiap Akun AWS anggota organisasi.

Versi API

Versi Referensi API Akun ini mendokumentasikan Account Management API versi 2021-02-01.

Note

Sebagai alternatif untuk menggunakan API secara langsung, Anda dapat menggunakan salah satu AWS SDK, yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa dan platform pemrograman (Java, Ruby, .NET, iOS, Android, dan lainnya). SDK menyediakan cara mudah untuk membuat akses terprogram ke Manajemen Akun. Misalnya, SDK menangani permintaan penandatanganan secara kriptografis, mengelola kesalahan, dan mencoba ulang permintaan secara otomatis. Untuk informasi selengkapnya tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat [Alat untuk Amazon Web Services](#).

Kami menyarankan Anda menggunakan AWS SDK untuk melakukan panggilan API terprogram ke layanan Manajemen Akun. Namun, Anda juga dapat menggunakan Account Management Query

API untuk melakukan panggilan langsung ke layanan web Manajemen Akun. Untuk mempelajari lebih lanjut tentang API Kueri Manajemen Akun, lihat [Memanggil API dengan membuat permintaan Kueri HTTP](#) di Panduan Pengguna Manajemen Akun. Manajemen Akun mendukung permintaan GET dan POST untuk semua tindakan. Artinya, API tidak mewajibkan Anda menggunakan GET untuk beberapa tindakan dan POST untuk yang lainnya. Namun, permintaan GET harus memenuhi ukuran batas dari sebuah URL. Oleh karena itu, untuk operasi yang membutuhkan ukuran lebih besar, gunakan permintaan POST.

Permintaan penandatanganan

Ketika Anda mengirim permintaan HTTP ke AWS, Anda harus menandatangani permintaan sehingga AWS dapat mengidentifikasi siapa yang mengirimnya. Anda menandatangani permintaan dengan kunci AWS akses Anda, yang terdiri dari ID kunci akses dan kunci akses rahasia. Kami sangat menyarankan agar Anda tidak membuat kunci akses untuk akun root Anda. Siapa pun yang memiliki kunci akses untuk akun root Anda memiliki akses tidak terbatas ke semua sumber daya di akun Anda. Sebagai gantinya, buat kunci akses untuk pengguna IAM yang memiliki hak administratif. Sebagai opsi lain, gunakan AWS Security Token Service untuk menghasilkan kredensi keamanan sementara, dan gunakan kredensial tersebut untuk menandatangani permintaan.

Untuk menandatangani permintaan, kami sarankan Anda menggunakan Signature Version 4. Jika Anda memiliki aplikasi yang sudah ada yang menggunakan Signature Version 2, Anda tidak perlu memperbaruinya untuk menggunakan Signature Version 4. Namun, beberapa operasi sekarang memerlukan Signature Version 4. Dokumentasi untuk operasi yang memerlukan versi 4 menunjukkan persyaratan ini. Untuk informasi selengkapnya, lihat [Menandatangani permintaan AWS API](#) di Panduan Pengguna IAM.

Saat Anda menggunakan AWS Command Line Interface (AWS CLI) atau salah satu AWS SDK untuk membuat permintaan AWS, alat ini secara otomatis menandatangani permintaan untuk Anda dengan kunci akses yang Anda tentukan saat Anda mengonfigurasi alat.

Support dan umpan balik untuk Account Management

Kami menyambut umpan balik Anda. Kirim komentar Anda ke feedback-awsaccounts@amazon.com atau posting umpan balik dan pertanyaan Anda di [forum dukungan Manajemen Akun](#). Untuk informasi selengkapnya tentang forum AWS dukungan, lihat [Bantuan Forum](#).

Bagaimana contoh disajikan

JSON yang dikembalikan oleh Manajemen Akun dalam menanggapi permintaan Anda adalah string panjang tunggal tanpa jeda baris atau spasi pemformatan. Baik jeda baris dan spasi putih ditampilkan

dalam contoh dalam panduan ini untuk meningkatkan keterbacaan. Ketika parameter input contoh juga akan menghasilkan string panjang yang akan melampaui layar, kami menyisipkan jeda baris untuk meningkatkan keterbacaan. Anda harus selalu mengirimkan input sebagai string teks JSON tunggal.

Merekam Permintaan API

Manajemen Akun mendukung CloudTrail, layanan yang merekam panggilan AWS API untuk Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan mana yang berhasil dibuat untuk Manajemen Akun, siapa yang membuat permintaan, kapan dibuat, dan sebagainya. Untuk informasi lebih lanjut tentang Manajemen Akun dan dukungannya CloudTrail, lihat [Logging AWS Account Management API menggunakan AWS CloudTrail](#). Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengaktifkannya dan menemukan file log Anda, lihat [Panduan AWS CloudTrail Pengguna](#).

Tindakan

Tindakan berikut didukung:

- [AcceptPrimaryEmailUpdate](#)
- [DeleteAlternateContact](#)
- [DisableRegion](#)
- [EnableRegion](#)
- [GetAccountInformation](#)
- [GetAlternateContact](#)
- [GetContactInformation](#)
- [GetGovCloudAccountInformation](#)
- [GetPrimaryEmail](#)
- [GetRegionOptStatus](#)
- [ListRegions](#)
- [PutAccountName](#)
- [PutAlternateContact](#)
- [PutContactInformation](#)
- [StartPrimaryEmailUpdate](#)

AcceptPrimaryEmailUpdate

Menerima permintaan yang berasal dari [StartPrimaryEmailUpdate](#) untuk memperbarui alamat email utama (juga dikenal sebagai alamat email pengguna root) untuk akun yang ditentukan.

Minta Sintaks

```
POST /acceptPrimaryEmailUpdate HTTP/1.1
Content-type: application/json
```

```
{
  "AccountId": "string",
  "Otp": "string",
  "PrimaryEmail": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

[AccountId](#)

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Operasi ini hanya dapat dipanggil dari akun manajemen atau akun administrator yang didelegasikan dari organisasi untuk akun anggota.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`.

Tipe: String

Pola: \d{12}

Wajib: Ya

Otp

Kode OTP dikirim ke yang `PrimaryEmail` ditentukan pada panggilan `StartPrimaryEmailUpdate` API.

Tipe: String

Pola: [a-zA-Z0-9]{6}

Wajib: Ya

PrimaryEmail

Alamat email utama baru untuk digunakan dengan akun yang ditentukan. Ini harus cocok dengan `PrimaryEmail` dari panggilan `StartPrimaryEmailUpdate` API.

Tipe: String

Kendala Panjang: Panjang minimum 5. Panjang maksimum 64.

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "Status": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Status

Mengambil status permintaan pembaruan email utama yang diterima.

Tipe: String

Nilai yang Valid: PENDING | ACCEPTED

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

ConflictException

Permintaan tidak dapat diproses karena konflik dalam status sumber daya saat ini. Misalnya, ini terjadi jika Anda mencoba mengaktifkan Wilayah yang saat ini sedang dinonaktifkan (dalam status `DISABLING`) atau jika Anda mencoba mengubah email pengguna root akun ke alamat email yang sudah digunakan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 409

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

DeleteAlternateContact

Menghapus kontak alternatif yang ditentukan dari file Akun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak alternatif, lihat [Memperbarui kontak alternatif untuk Anda Akun AWS](#).

Note

Sebelum Anda dapat memperbarui informasi kontak alternatif untuk informasi Akun AWS yang dikelola oleh AWS Organizations, Anda harus terlebih dahulu mengaktifkan integrasi antara Manajemen AWS Akun dan Organizations. Untuk informasi selengkapnya, lihat [Mengaktifkan akses tepercaya untuk Manajemen AWS Akun](#).

Minta Sintaks

```
POST /deleteAlternateContact HTTP/1.1
Content-type: application/json
```

```
{
  "AccountId": "string",
  "AlternateContactType": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan


Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun](#) administrator yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [administrator yang didelegasikan](#) ditetapkan.

 Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau ubah.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

[AlternateContactType](#)

Menentukan mana dari kontak alternatif untuk menghapus.

Tipe: String

Nilai yang Valid: BILLING | OPERATIONS | SECURITY

Wajib: Ya

Sintaxis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerError

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

`fieldList`

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut menghapus kontak alternatif keamanan untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact

{
  "AccountName": "MyAccount"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Contoh 2

Contoh berikut menghapus kontak alternatif penagihan untuk akun anggota yang ditentukan dalam suatu organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.DeleteAlternateContact
```

```
{
  "AccountId": "123456789012",
  "AlternateContactType": "BILLING"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

DisableRegion

Menonaktifkan (opts-out) Wilayah tertentu untuk akun.

Note

Tindakan menonaktifkan suatu Wilayah akan menghapus semua akses IAM ke sumber daya apa pun yang berada di Wilayah tersebut.

Minta Sintaks

```
POST /disableRegion HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "RegionName": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, parameter ini default ke akun Amazon Web Services dari identitas yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

RegionName

Menentukan Region-kode untuk nama Region tertentu (misalnya, `af-south-1`). Saat Anda menonaktifkan Wilayah, AWS lakukan tindakan untuk menonaktifkan Wilayah tersebut di akun Anda, seperti menghancurkan sumber daya IAM di Wilayah. Proses ini memerlukan waktu beberapa menit untuk sebagian besar akun, tetapi dapat memakan waktu beberapa jam. Anda tidak dapat mengaktifkan Wilayah sampai proses penonaktifan selesai sepenuhnya.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

Sintaxis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

ConflictException

Permintaan tidak dapat diproses karena konflik dalam status sumber daya saat ini. Misalnya, ini terjadi jika Anda mencoba mengaktifkan Wilayah yang saat ini sedang dinonaktifkan (dalam status `DISABLING`) atau jika Anda mencoba mengubah email pengguna root akun ke alamat email yang sudah digunakan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 409

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

EnableRegion

Mengaktifkan (opts-in) Wilayah tertentu untuk akun.

Minta Sintaks

```
POST /enableRegion HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "RegionName": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, parameter ini default ke akun Amazon Web Services dari identitas yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun](#) administrator yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiriAccountId. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan AccountId parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

RegionName

Menentukan Region-kode untuk nama Region tertentu (misalnya, `af-south-1`). Saat mengaktifkan Wilayah, AWS lakukan tindakan untuk mempersiapkan akun Anda di Wilayah tersebut, seperti mendistribusikan sumber daya IAM ke Wilayah. Proses ini memakan waktu beberapa menit untuk sebagian besar akun, tetapi bisa memakan waktu beberapa jam. Anda tidak dapat menggunakan Wilayah sampai proses ini selesai. Selain itu, Anda tidak dapat menonaktifkan Wilayah hingga proses pengaktifan selesai sepenuhnya.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

ConflictException

Permintaan tidak dapat diproses karena konflik dalam status sumber daya saat ini. Misalnya, ini terjadi jika Anda mencoba mengaktifkan Wilayah yang saat ini sedang dinonaktifkan (dalam status `DISABLING`) atau jika Anda mencoba mengubah email pengguna root akun ke alamat email yang sudah digunakan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 409

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

`fieldList`

Bidang tempat entri yang tidak valid terdeteksi.

`message`

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

`reason`

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

GetAccountInformation

Mengambil informasi tentang akun yang ditentukan termasuk nama akun, ID akun, tanggal dan waktu pembuatan akun, dan status akun. Untuk menggunakan API ini, pengguna atau peran IAM harus memiliki izin `account:GetAccountInformation` IAM.

Minta Sintaks

```
POST /getAccountInformation HTTP/1.1
Content-type: application/json

{
  "AccountId": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses terpercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [administrator yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontakannya ingin Anda ambil atau ubah.

Tipe: String

Pola: `\d{12}`

Diperlukan: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountCreatedDate": "string",
  "AccountId": "string",
  "AccountName": "string",
  "AccountState": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AccountCreatedDate

Tanggal dan waktu akun dibuat.

Tipe: Timestamp

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Operasi ini hanya dapat dipanggil dari akun manajemen atau akun administrator yang didelegasikan dari organisasi untuk akun anggota.

Note

Akun manajemen tidak dapat menentukan sendiri AccountId.

Tipe: String

Pola: `\d{12}`

AccountName

Nama akun.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Pola: `[- ; = ? - ~] +`

AccountState

Keadaan akun. Setiap status akun mewakili fase tertentu dalam siklus hidup akun. Gunakan informasi ini untuk mengelola akses akun, mengotomatiskan alur kerja, atau memicu tindakan berdasarkan perubahan status akun.

Nilai yang valid: PENDING_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

Tipe: String

Nilai yang Valid: PENDING_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut mengambil informasi akun untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAccountInformation

{}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "AccountId": "123456789012",
  "AccountName": "MyAccount",
  "AccountCreateDate": "2020-11-30T17:44:37Z",
  "AccountState": "ACTIVE"
}
```

Contoh 2

Contoh berikut mengambil informasi akun untuk akun anggota yang ditentukan dalam suatu organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAccountInformation

{
  "AccountId": "123456789012"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "AccountId": "123456789012",
```

```
"AccountName": "MyMemberAccount",  
"AccountCreatedDate": "2020-11-30T17:44:37Z",  
"AccountState": "ACTIVE"  
}
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

GetAlternateContact

Mengambil kontak alternatif yang ditentukan yang dilampirkan ke file Akun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak alternatif, lihat [Memperbarui kontak alternatif untuk Anda Akun AWS](#).

Note

Sebelum Anda dapat memperbarui informasi kontak alternatif untuk informasi Akun AWS yang dikelola oleh AWS Organizations, Anda harus terlebih dahulu mengaktifkan integrasi antara Manajemen AWS Akun dan Organizations. Untuk informasi selengkapnya, lihat [Mengaktifkan akses tepercaya untuk Manajemen AWS Akun](#).

Minta Sintaks

```
POST /getAlternateContact HTTP/1.1
```

```
Content-type: application/json
```

```
{  
  "AccountId": "string",  
  "AlternateContactType": "string"  
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan


Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun](#) administrator yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [administrator yang didelegasikan](#) ditetapkan.

 Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontakannya ingin Anda ambil atau ubah.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

[AlternateContactType](#)

Menentukan kontak alternatif yang ingin Anda ambil.

Tipe: String

Nilai yang Valid: BILLING | OPERATIONS | SECURITY

Wajib: Ya

Sintaxis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "AlternateContact": {
    "AlternateContactType": "string",
    "EmailAddress": "string",
```

```
    "Name": "string",  
    "PhoneNumber": "string",  
    "Title": "string"  
  }  
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AlternateContact

Struktur yang berisi rincian untuk kontak alternatif yang ditentukan.

Tipe: Objek AlternateContact

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat Jenis Kesalahan Umum.

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerError

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan validasi gagal.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut mengambil kontak alternatif keamanan untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact
```

```
{
  "AlternateContactType":"SECURITY"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "AlternateContact":{
    "Name":"Anika",
    "Title":"COO",
    "EmailAddress":"anika@example.com",
    "PhoneNumber":"206-555-0198",
    "AlternateContactType":"Security"
  }
}
```

Contoh 2

Contoh berikut mengambil kontak alternatif operasi untuk akun anggota tertentu dalam organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetAlternateContact

{
  "AccountId":"123456789012",
  "AlternateContactType":"Operations"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "AlternateContact":{
```

```
    "Name": "Anika",
    "Title": "C00",
    "EmailAddress": "anika@example.com",
    "PhoneNumber": "206-555-0198",
    "AlternateContactType": "Operations"
  }
}
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

GetContactInformation

Mengambil informasi kontak utama dari file. Akun AWS

Untuk detail selengkapnya tentang cara menggunakan operasi kontak utama, lihat [Memperbarui kontak utama untuk Anda Akun AWS](#).

Minta Sintaks

```
POST /getContactInformation HTTP/1.1
Content-type: application/json

{
  "AccountId": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

[AccountId](#)

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, parameter ini default ke akun Amazon Web Services dari identitas yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun](#) administrator yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontakannya ingin Anda ambil atau modifikasi.

Tipe: String

Pola: \d{12}

Diperlukan: Tidak

Sintaxis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "ContactInformation": {
    "AddressLine1": "string",
    "AddressLine2": "string",
    "AddressLine3": "string",
    "City": "string",
    "CompanyName": "string",
    "CountryCode": "string",
    "DistrictOrCounty": "string",
    "FullName": "string",
    "PhoneNumber": "string",
    "PostalCode": "string",
    "StateOrRegion": "string",
    "WebsiteUrl": "string"
  }
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

ContactInformation

Berisi rincian informasi kontak utama yang terkait dengan file Akun AWS.

Tipe: Objek [ContactInformation](#)

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

GetGovCloudAccountInformation

Mengambil informasi tentang GovCloud akun yang ditautkan ke akun standar yang ditentukan (jika ada) termasuk ID GovCloud akun dan status. Untuk menggunakan API ini, pengguna atau peran IAM harus memiliki izin `account:GetGovCloudAccountInformation` IAM.

Minta Sintaks

```
POST /getGovCloudAccountInformation HTTP/1.1
Content-type: application/json

{
  "StandardAccountId": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

StandardAccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun](#) administrator yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses terpercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [administrator yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan `sendiriAccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau ubah.

Tipe: String

Pola: \d{12}

Diperlukan: Tidak

Sintaxis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "AccountState": "string",
  "GovCloudAccountId": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

AccountState

Status akun dari GovCloud akun yang ditautkan.

Tipe: String

Nilai yang Valid: PENDING_ACTIVATION | ACTIVE | SUSPENDED | CLOSED

GovCloudAccountId

Nomor ID akun 12 digit dari GovCloud akun yang ditautkan.

Tipe: String

Pola: \d{12}

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerError

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 404

ResourceUnavailableException

Operasi gagal karena ditentukan sumber daya yang saat ini tidak tersedia.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 424

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut mengambil informasi GovCloud akun tertaut untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.GetGovCloudAccountInformation
{}

```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
{

```

```
"GovCloudAccountId": "123456789012",  
"AccountState": "ACTIVE"  
}
```

Contoh 2

Contoh berikut mengambil informasi GovCloud akun tertaut untuk akun anggota yang ditentukan dalam suatu organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Permintaan Sampel

```
POST / HTTP/1.1  
X-Amz-Target: AWSAccountV20210201.GetGovCloudAccountInformation  
  
{  
  "StandardAccountId": "111111111111"  
}
```

Contoh Respons

```
HTTP/1.1 200 OK  
Content-Type: application/json  
  
{  
  "GovCloudAccountId": "123456789012",  
  "AccountState": "ACTIVE"  
}
```

Contoh 3

Contoh berikut mencoba untuk mengambil informasi GovCloud akun tertaut untuk akun standar yang tidak ditautkan ke GovCloud akun.

Permintaan Sampel

```
POST / HTTP/1.1  
X-Amz-Target: AWSAccountV20210201.GetGovCloudAccountInformation  
  
{  
  "StandardAccountId": "222222222222"  
}
```

```
}
```

Contoh Respons

```
HTTP/1.1 404
Content-Type: application/json

{
  "message": "GovCloud Account ID not found for Standard Account - 222222222222."
}
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

GetPrimaryEmail

Mengambil alamat email utama untuk akun yang ditentukan.

Minta Sintaks

```
POST /getPrimaryEmail HTTP/1.1
Content-type: application/json

{
  "AccountId": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Operasi ini hanya dapat dipanggil dari akun manajemen atau akun administrator yang didelegasikan dari organisasi untuk akun anggota.

Note

Akun manajemen tidak dapat menentukan sendiriAccountId.

Tipe: String

Pola: \d{12}

Diperlukan: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "PrimaryEmail": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

PrimaryEmail

Mengambil alamat email utama yang terkait dengan akun yang ditentukan.

Tipe: String

Kendala Panjang: Panjang minimum 5. Panjang maksimum 64.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

GetRegionOptStatus

Mengambil status keikutsertaan dari Wilayah tertentu.

Minta Sintaks

```
POST /getRegionOptStatus HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "RegionName": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, parameter ini default ke akun Amazon Web Services dari identitas yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiriAccountId. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan AccountId parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Tipe: String

Pola: \d{12}

Wajib: Tidak

RegionName

Menentukan Region-kode untuk nama Region tertentu (misalnya,). af-south-1 Fungsi ini akan mengembalikan status Wilayah apa pun yang Anda lewatkan ke parameter ini.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "RegionName": "string",
  "RegionOptStatus": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

RegionName

Kode Region yang diteruskan.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

RegionOptStatus

Salah satu status potensial yang dapat dialami Region (Diaktifkan, Mengaktifkan, Dinonaktifkan, Menonaktifkan, Enabled_By_Default).

Tipe: String

Nilai yang Valid: ENABLED | ENABLING | DISABLING | DISABLED |
ENABLED_BY_DEFAULT

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

errorType

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

ListRegions

Daftar semua Wilayah untuk akun tertentu dan status keikutsertaannya masing-masing. Secara opsional, daftar ini dapat difilter oleh `region-opt-status-contains` parameter.

Minta Sintaks

```
POST /listRegions HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "MaxResults": number,
  "NextToken": "string",
  "RegionOptStatusContains": [ "string" ]
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, parameter ini default ke akun Amazon Web Services dari identitas yang digunakan untuk memanggil operasi. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau modifikasi.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

MaxResults

Jumlah total item yang akan dikembalikan dalam output perintah. Jika jumlah total item yang tersedia lebih dari nilai yang ditentukan, a `NextToken` disediakan dalam output perintah. Untuk melanjutkan pemberian nomor halaman, berikan nilai `NextToken` dalam argumen `starting-token` dari perintah berikutnya. Jangan gunakan elemen `NextToken` respons langsung di luar AWS CLI. Untuk contoh penggunaan, lihat [Pagination](#) di Panduan Pengguna Antarmuka Baris AWS Perintah.

Tipe: Bilangan Bulat

Rentang yang Valid: Nilai minimum 1. Nilai maksimum 50.

Wajib: Tidak

NextToken

Token yang digunakan untuk menentukan di mana harus memulai paginating. Ini adalah `NextToken` dari respons yang sebelumnya terpotong. Untuk contoh penggunaan, lihat [Pagination](#) di Panduan Pengguna Antarmuka Baris AWS Perintah.

Tipe: String

Batasan Panjang: Panjang minimum sebesar 0. Panjang maksimum sebesar 1000.

Wajib: Tidak

RegionOptStatusContains

Daftar status Region (Mengaktifkan, Diaktifkan, Menonaktifkan, Dinonaktifkan, `Enabled_BY_DEFAULT`) untuk digunakan untuk memfilter daftar Wilayah untuk akun tertentu. Misalnya, meneruskan nilai `ENABLING` hanya akan mengembalikan daftar Wilayah dengan status Region `ENABLING`.

Tipe: Array string

Nilai yang Valid: ENABLED | ENABLING | DISABLING | DISABLED |
ENABLED_BY_DEFAULT

Wajib: Tidak

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "NextToken": "string",
  "Regions": [
    {
      "RegionName": "string",
      "RegionOptStatus": "string"
    }
  ]
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

[NextToken](#)

Jika ada lebih banyak data yang akan dikembalikan, ini akan diisi. Itu harus diteruskan ke parameter `next-token` permintaan `list-regions`.

Tipe: String

[Regions](#)

Ini adalah daftar Wilayah untuk akun tertentu, atau jika parameter yang difilter digunakan, daftar Wilayah yang cocok dengan kriteria filter yang ditetapkan dalam `filter` parameter.

Tipe: Array objek [Region](#)

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerError

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

`fieldList`

Bidang tempat entri yang tidak valid terdeteksi.

`message`

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

`reason`

Alasan validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

PutAccountName

Memperbarui nama akun yang ditentukan. Untuk menggunakan API ini, prinsipal IAM harus memiliki izin IAM. `account:PutAccountName`

Minta Sintaks

```
POST /putAccountName HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "AccountName": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses terpercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [administrator yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontaknya ingin Anda ambil atau ubah.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

AccountName

Nama akun.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Pola: `[- ; = ? - ~] +`

Diperlukan: Ya

Sintaksis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerError

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

`fieldList`

Bidang tempat entri yang tidak valid terdeteksi.

`message`

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

`reason`

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut memperbarui nama akun yang kredensialnya digunakan untuk memanggil operasi.

Permintaan Sampel

```
POST / HTTP/1.1
```

```
X-Amz-Target: AWSAccountV20210201.PutAccountName
```

```
{  
  "AccountName": "MyAccount"  
}
```

Contoh Respons

```
HTTP/1.1 200 OK  
Content-Type: application/json
```

Contoh 2

Contoh berikut memperbarui nama akun untuk akun anggota yang ditentukan dalam suatu organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Permintaan Sampel

```
POST / HTTP/1.1  
X-Amz-Target: AWSAccountV20210201.PutAccountName
```

```
{  
  "AccountId": "123456789012",  
  "AccountName": "MyMemberAccount"  
}
```

Contoh Respons

```
HTTP/1.1 200 OK  
Content-Type: application/json
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

PutAlternateContact

Memodifikasi kontak alternatif yang ditentukan yang dilampirkan ke file Akun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak alternatif, lihat [Memperbarui kontak alternatif untuk Anda Akun AWS](#).

Note

Sebelum Anda dapat memperbarui informasi kontak alternatif untuk informasi Akun AWS yang dikelola oleh AWS Organizations, Anda harus terlebih dahulu mengaktifkan integrasi antara Manajemen AWS Akun dan Organizations. Untuk informasi selengkapnya, lihat [Mengaktifkan akses tepercaya untuk Manajemen AWS Akun](#).

Minta Sintaks

```
POST /putAlternateContact HTTP/1.1
```

```
Content-type: application/json
```

```
{
  "AccountId": "string",
  "AlternateContactType": "string",
  "EmailAddress": "string",
  "Name": "string",
  "PhoneNumber": "string",
  "Title": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan


Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun AWS akun yang ingin Anda akses atau modifikasi dengan operasi ini.

Jika Anda tidak menentukan parameter ini, itu default ke AWS akun identitas yang digunakan untuk memanggil operasi.

Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun](#) administrator yang didelegasikan, dan ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [administrator yang didelegasikan](#) ditetapkan.

 Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`; itu harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, maka jangan tentukan parameter ini, dan panggil operasi menggunakan identitas milik akun yang kontakannya ingin Anda ambil atau ubah.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

[AlternateContactType](#)

Menentukan kontak alternatif yang ingin Anda buat atau update.

Tipe: String

Nilai yang Valid: BILLING | OPERATIONS | SECURITY

Wajib: Ya

[EmailAddress](#)

Menentukan alamat email untuk kontak alternatif.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 254.

Pola: `[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*`

Wajib: Ya

Name

Menentukan nama untuk kontak alternatif.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum adalah 64.

Wajib: Ya

PhoneNumber

Menentukan nomor telepon untuk kontak alternatif.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 25.

Pola: `[\s0-9()+-]+`

Wajib: Ya

Title

Menentukan judul untuk kontak alternatif.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

Sintaxis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerError

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

`fieldList`

Bidang tempat entri yang tidak valid terdeteksi.

`message`

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

`reason`

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Contoh

Contoh 1

Contoh berikut menetapkan kontak alternatif penagihan untuk akun yang kredensialnya digunakan untuk memanggil operasi.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
  "AlternateContactType": "Billing",
  "Name": "Carlos Salazar",
  "Title": "CF0",
  "EmailAddress": "carlos@example.com",
  "PhoneNumber": "206-555-0199"
}
```

Contoh Respons

```
HTTP/1.1 200 OK
Content-Type: application/json
```

Contoh 2

Contoh berikut menetapkan atau menimpa kontak alternatif penagihan untuk akun anggota yang ditentukan dalam organisasi. Anda harus menggunakan kredensi dari akun manajemen organisasi atau dari akun admin yang didelegasikan oleh layanan Manajemen Akun.

Permintaan Sampel

```
POST / HTTP/1.1
X-Amz-Target: AWSAccountV20210201.PutAlternateContact

{
  "AccountId": "123456789012",
  "AlternateContactType": "Billing",
}
```

```
"Name": "Carlos Salazar",  
"Title": "CFO",  
"EmailAddress": "carlos@example.com",  
"PhoneNumber": "206-555-0199"  
}
```

Contoh Respons

```
HTTP/1.1 200 OK  
Content-Type: application/json
```

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

PutContactInformation

Memperbarui informasi kontak utama dari file Akun AWS.

Untuk detail selengkapnya tentang cara menggunakan operasi kontak utama, lihat [Memperbarui kontak utama untuk Anda Akun AWS](#).

Minta Sintaks

```
POST /putContactInformation HTTP/1.1
Content-type: application/json
```

```
{
  "AccountId": "string",
  "ContactInformation": {
    "AddressLine1": "string",
    "AddressLine2": "string",
    "AddressLine3": "string",
    "City": "string",
    "CompanyName": "string",
    "CountryCode": "string",
    "DistrictOrCounty": "string",
    "FullName": "string",
    "PhoneNumber": "string",
    "PostalCode": "string",
    "StateOrRegion": "string",
    "WebsiteUrl": "string"
  }
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

[AccountId](#)

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Jika Anda tidak menentukan parameter ini, parameter ini default ke akun Amazon Web Services dari identitas yang digunakan untuk memanggil operasi. Untuk menggunakan parameter

ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [administrator yang didelegasikan](#) ditetapkan.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`. Ini harus memanggil operasi dalam konteks mandiri dengan tidak menyertakan `AccountId` parameter.

Untuk memanggil operasi ini pada akun yang bukan anggota organisasi, jangan tentukan parameter ini. Sebagai gantinya, panggil operasi menggunakan identitas milik akun yang kontakannya ingin Anda ambil atau modifikasi.

Tipe: String

Pola: `\d{12}`

Wajib: Tidak

[ContactInformation](#)

Berisi rincian informasi kontak utama yang terkait dengan file Akun AWS.

Tipe: Objek [ContactInformation](#)

Wajib: Ya

Sintaxis Respons

```
HTTP/1.1 200
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200 dengan isi HTTP kosong.

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

InternalServerError

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

`fieldList`

Bidang tempat entri yang tidak valid terdeteksi.

`message`

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

`reason`

Alasan validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

StartPrimaryEmailUpdate

Memulai proses untuk memperbarui alamat email utama untuk akun yang ditentukan.

Minta Sintaks

```
POST /startPrimaryEmailUpdate HTTP/1.1
Content-type: application/json

{
  "AccountId": "string",
  "PrimaryEmail": "string"
}
```

Parameter Permintaan URI

Permintaan tidak menggunakan parameter URI apa pun.

Isi Permintaan

Permintaan menerima data berikut dalam format JSON.

AccountId

Menentukan 12 digit nomor ID akun Akun AWS yang ingin Anda akses atau modifikasi dengan operasi ini. Untuk menggunakan parameter ini, pemanggil harus berupa identitas di [akun manajemen organisasi atau akun administrator](#) yang didelegasikan. ID akun yang ditentukan harus berupa akun anggota di organisasi yang sama. Organisasi harus mengaktifkan [semua fitur, dan organisasi harus mengaktifkan akses tepercaya](#) untuk layanan Manajemen Akun, dan secara opsional akun [admin yang didelegasikan](#) ditetapkan.

Operasi ini hanya dapat dipanggil dari akun manajemen atau akun administrator yang didelegasikan dari organisasi untuk akun anggota.

Note

Akun manajemen tidak dapat menentukan sendiri `AccountId`.

Tipe: String

Pola: \d{12}

Wajib: Ya

PrimaryEmail

Alamat email utama baru (juga dikenal sebagai alamat email pengguna root) untuk digunakan dalam akun yang ditentukan.

Tipe: String

Kendala Panjang: Panjang minimum 5. Panjang maksimum 64.

Wajib: Ya

Sintaksis Respons

```
HTTP/1.1 200
Content-type: application/json

{
  "Status": "string"
}
```

Elemen Respons

Jika tindakan berhasil, layanan mengirimkan kembali respons HTTP 200.

Layanan mengembalikan data berikut dalam format JSON.

Status

Status permintaan pembaruan email utama.

Tipe: String

Nilai yang Valid: PENDING | ACCEPTED

Kesalahan

Untuk informasi tentang kesalahan yang umum untuk semua tindakan, lihat [Jenis Kesalahan Umum](#).

AccessDeniedException

Operasi gagal karena identitas panggilan tidak memiliki izin minimum yang diperlukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 403

ConflictException

Permintaan tidak dapat diproses karena konflik dalam status sumber daya saat ini. Misalnya, ini terjadi jika Anda mencoba mengaktifkan Wilayah yang saat ini sedang dinonaktifkan (dalam status `DISABLING`) atau jika Anda mencoba mengubah email pengguna root akun ke alamat email yang sudah digunakan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 409

InternalServerErrorException

Operasi gagal karena kesalahan internal ke AWS. Coba operasi Anda lagi nanti.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 500

ResourceNotFoundException

Operasi gagal karena menentukan sumber daya yang tidak dapat ditemukan.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 404

TooManyRequestsException

Operasi gagal karena dipanggil terlalu sering dan melebihi batas throttle.

`errorType`

Nilai diisi ke header `x-amzn-ErrorType` respons oleh API Gateway.

Kode Status HTTP: 429

ValidationException

Operasi gagal karena salah satu parameter input tidak valid.

fieldList

Bidang tempat entri yang tidak valid terdeteksi.

message

Pesan yang memberi tahu Anda tentang apa yang tidak valid tentang permintaan tersebut.

reason

Alasan mengapa validasi gagal.

Kode Status HTTP: 400

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS Antarmuka Baris Perintah V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK untuk V3 JavaScript](#)
- [AWS SDK para Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK untuk Python](#)
- [AWS SDK for Ruby V3](#)

Tindakan terkait di AWS layanan lain

Operasi berikut terkait dengan AWS Account Management tetapi merupakan bagian dari AWS Organizations namespace:

- [CreateAccount](#)
- [CreateGovCloudAccount](#)
- [DescribeAccount](#)

CreateAccount

Operasi `CreateAccount` API tersedia untuk digunakan hanya dalam konteks organisasi yang dikelola oleh AWS Organizations layanan. Operasi API didefinisikan dalam namespace layanan tersebut.

Untuk informasi selengkapnya, lihat [CreateAccount](#) dalam Referensi API AWS Organizations .

CreateGovCloudAccount

Operasi `CreateGovCloudAccount` API tersedia untuk digunakan hanya dalam konteks organisasi yang dikelola oleh AWS Organizations layanan. Operasi API didefinisikan dalam namespace layanan tersebut.

Untuk informasi selengkapnya, lihat [CreateGovCloudAccount](#) dalam Referensi API AWS Organizations .

DescribeAccount

Operasi `DescribeAccount` API tersedia untuk digunakan hanya dalam konteks organisasi yang dikelola oleh AWS Organizations layanan. Operasi API didefinisikan dalam namespace layanan tersebut.

Untuk informasi selengkapnya, lihat [DescribeAccount](#) dalam Referensi API AWS Organizations .

Tipe Data

tipe data berikut didukung:

- [AlternateContact](#)
- [ContactInformation](#)
- [Region](#)
- [ValidationExceptionField](#)

AlternateContact

Struktur yang berisi rincian kontak alternatif yang terkait dengan AWS akun

Daftar Isi

AlternateContactType

Jenis kontak alternatif.

Tipe: String

Nilai yang Valid: BILLING | OPERATIONS | SECURITY

Wajib: Tidak

EmailAddress

Alamat email yang terkait dengan kontak alternatif ini.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 254.

Pola: `[\s]*[\w+=.#!&-]+@[\w.-]+\.[\w]+[\s]*`

Wajib: Tidak

Name

Nama yang terkait dengan kontak alternatif ini.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum adalah 64.

Wajib: Tidak

PhoneNumber

Nomor telepon yang terkait dengan kontak alternatif ini.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 25.

Pola: `[\s0-9()+-]+`

Wajib: Tidak

Title

Judul yang terkait dengan kontak alternatif ini.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ContactInformation

Berisi rincian informasi kontak utama yang terkait dengan file Akun AWS.

Daftar Isi

AddressLine1

Baris pertama dari alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 60.

Wajib: Ya

City

Kota alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

CountryCode

Kode negara dua huruf ISO-3166 untuk alamat kontak utama.

Tipe: String

Kendala Panjang: Panjang tetap 2.

Wajib: Ya

FullName

Nama lengkap alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Ya

PhoneNumber

Nomor telepon dari informasi kontak utama. Nomor tersebut akan divalidasi dan, di beberapa negara, diperiksa untuk aktivasi.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 20.

Pola: `[+][\s0-9()-]+`

Wajib: Ya

PostalCode

Kode pos dari alamat kontak utama.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 20.

Wajib: Ya

AddressLine2

Baris kedua dari alamat kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 60.

Wajib: Tidak

AddressLine3

Baris ketiga dari alamat kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 60.

Wajib: Tidak

CompanyName

Nama perusahaan yang terkait dengan informasi kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Tidak

DistrictOrCounty

Distrik atau kabupaten dari alamat kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Tidak

StateOrRegion

Negara bagian atau wilayah alamat kontak utama. Jika alamat surat berada di Amerika Serikat (AS), nilai dalam bidang ini dapat berupa kode status dua karakter (misalnya,NJ) atau nama negara lengkap (misalnya,New Jersey). Bidang ini diperlukan di negara-negara berikut:US,CA,GB,DE,JP,IN, danBR.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Tidak

WebsiteUrl

URL situs web yang terkait dengan informasi kontak utama, jika ada.

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 256.

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Region

Ini adalah struktur yang menyatakan Wilayah untuk akun tertentu, yang terdiri dari nama dan status keikutsertaan.

Daftar Isi

RegionName

Kode Region dari Region tertentu (misalnya, `us-east-1`).

Tipe: String

Batasan Panjang: Panjang minimum 1. Panjang maksimum 50.

Wajib: Tidak

RegionOptStatus

Salah satu status potensial yang dapat dialami Region (Diaktifkan, Mengaktifkan, Dinonaktifkan, Menonaktifkan, `Enabled_By_Default`).

Tipe: String

Nilai yang Valid: `ENABLED` | `ENABLING` | `DISABLING` | `DISABLED` | `ENABLED_BY_DEFAULT`

Wajib: Tidak

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ValidationExceptionField

Masukan gagal memenuhi kendala yang ditentukan oleh AWS layanan di bidang tertentu.

Daftar Isi

message

Pesan tentang pengecualian validasi.

Tipe: String

Diperlukan: Ya

name

Nama bidang tempat entri yang tidak valid terdeteksi.

Tipe: String

Wajib: Ya

Lihat Juga

Untuk informasi selengkapnya tentang penggunaan API ini di salah satu bahasa khusus AWS SDKs, lihat berikut ini:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Parameter Umum

Daftar berikut berisi parameter yang digunakan semua tindakan untuk menandatangani permintaan Tanda Tangan Versi 4 dengan string kueri. Setiap parameter khusus tindakan tercantum dalam topik untuk tindakan tersebut. Untuk informasi selengkapnya tentang Tanda Tangan Versi 4, lihat [Menandatangani permintaan AWS API](#) di Panduan Pengguna IAM.

X-Amz-Algorithm

Algoritme hash yang Anda gunakan untuk membuat tanda tangan permintaan.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Nilai yang Valid: AWS4-HMAC-SHA256

Diperlukan: Kondisional

X-Amz-Credential

Nilai lingkup kredensial, yang merupakan string yang menyertakan access key Anda, tanggal, wilayah yang Anda targetkan, layanan yang Anda minta, dan string penghentian ("aws4_request"). Nilai dinyatakan dalam format berikut: access_key/HHBBTTTT/wilayah/layanan/aws4_request.

Untuk informasi selengkapnya, lihat [Membuat permintaan AWS API yang ditandatangani](#) di Panduan Pengguna IAM.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Wajib: Bersyarat

X-Amz-Date

Tanggal yang digunakan untuk membuat tanda tangan. Format harus berupa format dasar ISO 8601 (YYYYMMDD'T'HMMSS'Z'). Misalnya, waktu tanggal berikut adalah X-Amz-Date nilai yang valid:20120325T120000Z.

Syarat: X-Amz-Date bersifat opsional untuk semua permintaan; ini dapat digunakan untuk menimpa tanggal yang digunakan untuk menandatangani permintaan. Jika header Tanggal ditentukan dalam format dasar ISO 8601, tidak X-Amz-Date diperlukan. Ketika X-Amz-Date digunakan, itu selalu mengesampingkan nilai header Tanggal. Untuk informasi selengkapnya, lihat [Elemen tanda tangan permintaan AWS API](#) di Panduan Pengguna IAM.

Jenis: string

Wajib: Bersyarat

X-Amz-Security-Token

Token keamanan sementara yang diperoleh melalui panggilan ke AWS Security Token Service (AWS STS). Untuk daftar layanan yang mendukung kredensi keamanan sementara AWS STS, lihat layanan [Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM](#).

Kondisi: Jika Anda menggunakan kredensi keamanan sementara dari AWS STS, Anda harus menyertakan token keamanan.

Jenis: string

Wajib: Bersyarat

X-Amz-Signature

Menentukan tanda tangan yang dikodekan oleh hex yang dihitung dari string to sign dan kunci penandatanganan turunan.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Wajib: Bersyarat

X-Amz-SignedHeaders

Menentukan semua header HTTP yang disertakan sebagai bagian dari permintaan kanonik. Untuk informasi selengkapnya tentang menentukan header yang ditandatangani, lihat [Membuat permintaan AWS API yang ditandatangani](#) di Panduan Pengguna IAM.

Syarat: Tentukan parameter ini ketika Anda menyertakan informasi autentikasi dalam string kueri alih-alih di header otorisasi HTTP.

Tipe: string

Diperlukan: Kondisional

Jenis Kesalahan Umum

Bagian ini mencantumkan jenis kesalahan umum yang mungkin dikembalikan oleh AWS layanan ini. Tidak semua layanan mengembalikan semua jenis kesalahan yang tercantum di sini. Untuk kesalahan khusus pada tindakan API untuk layanan ini, lihat topik untuk tindakan API tersebut.

AccessDeniedException

Anda tidak memiliki izin untuk melakukan tindakan ini. Verifikasi bahwa kebijakan IAM Anda menyertakan izin yang diperlukan.

Kode Status HTTP: 403

ExpiredTokenException

Token keamanan yang termasuk dalam permintaan telah kedaluwarsa. Minta token keamanan baru dan coba lagi.

Kode Status HTTP: 403

IncompleteSignature

Tanda tangan permintaan tidak sesuai dengan AWS standar. Verifikasi bahwa Anda menggunakan AWS kredensi yang valid dan permintaan Anda diformat dengan benar. Jika Anda menggunakan SDK, pastikan itu mutakhir.

Kode Status HTTP: 403

InternalFailure

Permintaan tidak dapat diproses sekarang karena masalah server internal. Coba lagi nanti. Jika masalah berlanjut, hubungi AWS Support.

Kode Status HTTP: 500

MalformedHttpRequestException

Badan permintaan tidak dapat diproses. Ini biasanya terjadi ketika badan permintaan tidak dapat didekompresi menggunakan algoritme pengkodean konten yang ditentukan. Verifikasi bahwa header pengkodean konten cocok dengan format kompresi yang digunakan.

Kode Status HTTP: 400

NotAuthorized

Anda tidak memiliki izin untuk melakukan tindakan ini. Verifikasi bahwa kebijakan IAM Anda menyertakan izin yang diperlukan.

Kode Status HTTP: 401

OptInRequired

AWS Akun Anda memerlukan langganan untuk layanan ini. Verifikasi bahwa Anda telah mengaktifkan layanan di akun Anda.

Kode Status HTTP: 403

RequestAbortedException

Permintaan dibatalkan sebelum tanggapan dapat dikembalikan. Ini biasanya terjadi ketika klien menutup koneksi.

Kode Status HTTP: 400

RequestEntityTooLargeException

Entitas permintaan terlalu besar. Kurangi ukuran badan permintaan dan coba lagi.

Kode Status HTTP: 413

RequestTimeoutException

Permintaan habis waktunya. Server tidak menerima permintaan lengkap dalam jangka waktu yang diharapkan. Coba lagi.

Kode Status HTTP: 408

ServiceUnavailable

Layanan untuk sementara tidak tersedia. Coba lagi nanti.

Kode Status HTTP: 503

ThrottlingException

Tingkat permintaan Anda terlalu tinggi. Permintaan coba ulang AWS SDKs secara otomatis yang menerima pengecualian ini. Kurangi frekuensi permintaan.

Kode Status HTTP: 400

UnknownOperationException

Tindakan atau operasi tidak dikenali. Verifikasi bahwa nama tindakan dieja dengan benar dan didukung oleh versi API yang Anda gunakan.

Kode Status HTTP: 404

UnrecognizedClientException

Sertifikat X.509 atau ID kunci AWS akses yang Anda berikan tidak ada dalam catatan kami. Verifikasi bahwa Anda menggunakan kredensi yang valid dan belum kedaluwarsa.

Kode Status HTTP: 403

ValidationError

Input tidak memenuhi format atau kendala yang diperlukan. Periksa apakah semua parameter yang diperlukan disertakan dan nilainya valid.

Kode Status HTTP: 400

Memanggil API dengan membuat permintaan Kueri HTTP

Bagian ini berisi informasi umum tentang penggunaan Query API for AWS Account Management. Untuk detail tentang operasi dan kesalahan API, lihat [Referensi API](#).

Note

Alih-alih melakukan panggilan langsung ke AWS Account Management Query API, Anda dapat menggunakan salah satunya AWS SDKs. AWS SDKs Terdiri dari perpustakaan dan kode sampel untuk berbagai bahasa pemrograman dan platform (Java, Ruby, .NET, iOS, Android, dan banyak lagi). SDKs Menyediakan cara mudah untuk membuat akses terprogram ke Manajemen AWS Akun dan AWS. Misalnya, SDKs menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang AWS SDKs, termasuk cara mengunduh dan menginstalnya, lihat [Alat untuk Amazon Web Services](#).

Dengan API Kueri untuk Manajemen AWS Akun, Anda dapat memanggil tindakan layanan. Permintaan API kueri adalah permintaan HTTPS yang harus berisi `Action` parameter untuk menunjukkan operasi yang akan dilakukan. AWS Manajemen Akun mendukung GET dan POST meminta semua operasi. Artinya, API tidak mengharuskan Anda untuk menggunakan GET untuk beberapa tindakan dan POST untuk tindakan lainnya. Namun, GET permintaan tunduk pada ukuran batasan URL. Meskipun batas ini bergantung pada browser, batas tipikal adalah 2.048 byte. Oleh karena itu, untuk permintaan Query API yang memerlukan ukuran lebih besar, Anda harus menggunakan POST permintaan.

Responsnya adalah dokumen XML. Untuk detail tentang respons, lihat halaman tindakan individual di halaman [Referensi API](#).

Topik

- [Titik akhir](#)
- [HTTPS diperlukan](#)
- [Menandatangani permintaan API Manajemen AWS Akun](#)

Titik akhir

AWS Manajemen Akun memiliki titik akhir API global tunggal yang di-host di AS Timur (Virginia N.). Wilayah AWS

Untuk informasi selengkapnya tentang AWS titik akhir dan Wilayah untuk semua layanan, lihat [Wilayah dan Titik Akhir](#) di Referensi Umum AWS

HTTPS diperlukan

Karena Query API dapat mengembalikan informasi sensitif seperti kredensi keamanan, Anda harus menggunakan HTTPS untuk mengenkripsi semua permintaan API.

Menandatangani permintaan API Manajemen AWS Akun

Permintaan harus ditandatangani menggunakan access key ID dan secret access key. Kami sangat menyarankan agar Anda tidak menggunakan kredensi akun AWS root Anda untuk pekerjaan sehari-hari dengan Manajemen AWS Akun. Anda dapat menggunakan kredensi untuk pengguna AWS Identity and Access Management (IAM) atau kredensial sementara seperti yang Anda gunakan dengan peran IAM.

Untuk menandatangani permintaan API, Anda harus menggunakan AWS Signature Version 4. Untuk selengkapnya tentang penggunaan Tanda Tangan Versi 4, lihat [Menandatangani permintaan AWS API](#) di Panduan Pengguna IAM.

Untuk informasi selengkapnya, lihat berikut ini:

- [AWS Security Credentials](#) — Memberikan informasi umum tentang jenis kredensial yang dapat Anda gunakan untuk mengakses. AWS
- [Praktik terbaik keamanan di IAM](#) — Menawarkan saran untuk menggunakan layanan IAM untuk membantu mengamankan AWS sumber daya Anda, termasuk yang ada di Manajemen AWS Akun.

- [Kredensial keamanan sementara di IAM](#) — Menjelaskan cara membuat dan menggunakan kredensial keamanan sementara.

Kuota untuk AWS Account Management

Anda Akun AWS memiliki kuota default, sebelumnya disebut sebagai batas, untuk setiap layanan. AWS Kecuali dinyatakan lain, setiap kuota adalah Wilayah AWS-spesifik.

Masing-masing Akun AWS memiliki kuota berikut yang terkait dengan Manajemen Akun.

Sumber daya	Kuota
Jumlah maksimum <code>StartPrimaryEmailUpdate</code> permintaan per akun target	3 per 30 detik
Jumlah kontak alternatif dalam sebuah Akun AWS	3 - masing-masing untuk <code>BILLING</code> , <code>SECURITY</code> , dan <code>OPERATIONS</code>
Jumlah permintaan pilihan wilayah bersamaan per akun	6
Jumlah permintaan pilihan wilayah bersamaan per organisasi	50
Tingkat <code>AcceptPrimaryEmailUpdate</code> permintaan per akun penelepon	1 per detik, meledak menjadi 1 per detik
Tarif <code>DeleteAlternateContact</code> permintaan per akun	1 per detik, meledak menjadi 6 per detik
Tarif <code>DisableRegion</code> permintaan per akun	1 per detik, meledak menjadi 1 per detik
Tarif <code>EnableRegion</code> permintaan per akun	1 per detik, meledak menjadi 1 per detik
Tingkat <code>GetAccountInformation</code> permintaan per akun penelepon	3 per detik, meledak menjadi 3 per detik
Tarif <code>GetAlternateContact</code> permintaan per akun	10 per detik, meledak menjadi 15 per detik
Tarif <code>GetContactInformation</code> permintaan per akun	10 per detik, meledak menjadi 15 per detik

Sumber daya	Kuota
Tarif GetGovCloudAccountInformation permintaan per akun	3 per detik, meledak menjadi 5 per detik
Tingkat GetPrimaryEmail permintaan per akun penelepon	3 per detik, meledak menjadi 3 per detik
Tarif GetRegionOptStatus permintaan per akun	5 per detik, meledak menjadi 5 per detik
Tarif ListRegions permintaan per akun	5 per detik, meledak menjadi 5 per detik
Tingkat PutAccountName permintaan per akun penelepon	1 per detik, meledak menjadi 1 per detik
Tarif PutAlternateContact permintaan per akun	5 per detik, meledak menjadi 8 per detik
Tarif PutContactInformation permintaan per akun	5 per detik, meledak menjadi 8 per detik
Tingkat StartPrimaryEmailUpdate permintaan per akun penelepon	1 per detik, meledak menjadi 1 per detik

Kelola akun di India

Jika Anda mendaftar untuk yang baru Akun AWS dan memilih India untuk kontak dan alamat penagihan Anda, perjanjian pengguna Anda adalah dengan Amazon Web Services India Private Limited (AWS India), AWS penjual lokal di India. AWS India mengelola tagihan Anda, dan total faktur Anda tercantum dalam rupee India (INR), bukan dolar AS (USD). Untuk informasi tentang mengelola Akun AWS, lihat [Konfigurasi Akun AWS](#).

Jika akun Anda AWS di India, ikuti prosedur dalam topik ini untuk mengelola akun Anda. Topik ini menjelaskan cara mendaftar untuk akun AWS India, mengedit informasi tentang akun AWS India Anda, mengelola verifikasi pelanggan, dan menambahkan atau mengedit Nomor Akun Permanen (PAN) Anda.

Sebagai bagian dari verifikasi kartu kredit saat mendaftar, AWS India menagih kartu kredit Anda 2 INR. AWS India mengembalikan 2 INR setelah verifikasi selesai. Anda mungkin akan dialihkan ke bank sebagai bagian dari proses verifikasi.

Topik

- [Buat sebuah Akun AWS dengan AWS India](#)
- [Kelola informasi verifikasi pelanggan Anda](#)

Buat sebuah Akun AWS dengan AWS India

AWS India adalah penjual lokal AWS di India. Jika kontak dan alamat penagihan Anda berada di India dan Anda ingin membuat akun, gunakan prosedur berikut untuk mendaftar akun AWS India.

Untuk mendaftar untuk AWS Akun India

1. Buka [halaman beranda Amazon Web Services](#).
2. Pilih Buat Akun AWS.


Note

Jika Anda masuk AWS baru-baru ini, opsi itu mungkin tidak ada. Sebagai gantinya, pilih Masuk ke Konsol. Jika Buat yang baru Akun AWS masih tidak terlihat, pilih Masuk ke akun lain, lalu pilih Buat yang baru Akun AWS.

3. Masukkan informasi akun Anda, verifikasi alamat email Anda, dan pilih kata sandi yang kuat untuk akun Anda.
4. Pilih Bisnis atau Pribadi. Akun pribadi dan akun bisnis memiliki fitur dan fungsi yang sama.
5. Masukkan informasi kontak perusahaan atau pribadi Anda. Jika kontak atau alamat penagihan Anda berbasis di India, sesuai dengan peraturan Tim Tanggap Darurat Komputer India (CERT-In), AWS diperlukan untuk mengumpulkan dan memvalidasi informasi identitas Anda sebelum memberi Anda akses ke layanan. AWS

Nama yang Anda pilih antara kontak atau informasi penagihan harus sama persis dengan nama yang muncul pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen. Untuk daftar jenis dokumen yang diterima, lihat [the section called “Dokumen India yang diterima untuk verifikasi pelanggan”](#).

6. Setelah Anda membaca perjanjian pelanggan, pilih kotak centang syarat dan ketentuan, lalu pilih Lanjutkan.
7. Pada halaman Informasi penagihan, masukkan metode pembayaran yang ingin Anda gunakan. Anda harus memberikan CVV Anda sebagai bagian dari proses verifikasi.
8. Di bawah Apakah Anda memiliki PAN? , pilih Ya jika Anda memiliki Nomor Rekening Permanen (PAN) yang ingin ditampilkan pada faktur pajak Anda, lalu masukkan PAN Anda. Jika Anda tidak memiliki PAN atau ingin menambahkannya setelah mendaftar, pilih No.
9. Pilih Verifikasi dan lanjutkan. AWS India menagih kartu Anda 2 INR sebagai bagian dari proses verifikasi. AWS India mengembalikan 2 INR setelah verifikasi selesai.
10. Pada halaman Konfirmasi identitas Anda, pilih tujuan utama pendaftaran akun Anda.
11. Pilih jenis kepemilikan yang paling mewakili pemilik akun. Jika Anda memilih perusahaan, organisasi, atau kemitraan sebagai jenis kepemilikan, masukkan nama orang manajerial kunci. Orang manajerial utama dapat menjadi direktur, kepala operasi, atau orang yang bertanggung jawab atas operasi dalam bisnis Anda.
12. Bergantung pada jenis kepemilikan yang Anda pilih, pilih jenis dokumen India yang diterima untuk digunakan untuk verifikasi dan ketikkan informasi dokumen Anda.

 Note

Jika Anda memiliki akun pribadi dan berencana untuk menggunakan SIM yang tidak dikeluarkan oleh Uni India, sebaiknya gunakan jenis dokumen pribadi yang berbeda untuk verifikasi.


13. Pilih nama yang ingin Anda gunakan untuk verifikasi pelanggan.

Nama-nama dari informasi penagihan dan kontak Anda akan muncul untuk dipilih jika dikaitkan dengan alamat India. Pastikan nama yang Anda pilih cocok dengan nama pada jenis dokumen yang akan digunakan untuk verifikasi pelanggan. Jika Anda perlu membuat perubahan pada nama yang terkait dengan tagihan atau alamat kontak Anda, Anda dapat melakukannya setelah Anda menyelesaikan pendaftaran akun.

14. Berikan persetujuan Anda untuk mengirimkan informasi untuk verifikasi, lalu pilih Lanjutkan.

Anda akan diberitahu tentang hasil verifikasi pelanggan melalui email setelah Anda menyelesaikan pendaftaran akun. Anda juga dapat memeriksa status pada halaman verifikasi Pelanggan di pengaturan akun Anda atau di Dasbor AWS Kesehatan nanti. Anda harus lulus verifikasi pelanggan untuk mengakses AWS layanan.

15. Pilih apakah Anda ingin memverifikasi nomor ponsel Anda melalui Pesan teks (SMS) atau Panggilan suara.
16. Pilih kode negara atau wilayah Anda, lalu masukkan nomor ponsel Anda.
17. Lengkapi pemeriksaan keamanan.
18. Pilih Kirim SMS atau Hubungi Saya Sekarang. Setelah beberapa saat, Anda akan menerima pin empat digit dalam SMS atau panggilan otomatis di ponsel Anda.
19. Pada halaman Konfirmasi identitas Anda, masukkan pin yang Anda terima dan pilih Lanjutkan.
20. Pada halaman Pilih paket dukungan, pilih paket dukungan Anda, lalu pilih Daftar lengkap. Setelah metode pembayaran dan verifikasi pelanggan Anda diverifikasi, akun Anda akan diaktifkan dan Anda akan menerima email yang mengonfirmasi aktivasi akun Anda.

 Note

Jika Anda telah menyelesaikan verifikasi pelanggan dan mengedit nama, alamat, atau dokumen yang sebelumnya digunakan untuk memverifikasi identitas Anda, Anda mungkin perlu memperbarui dan menyelesaikan verifikasi pelanggan Anda lagi. Untuk

informasi selengkapnya, lihat [the section called “Mengedit informasi verifikasi pelanggan Anda”](#).

Kelola informasi verifikasi pelanggan Anda

Sesuai dengan peraturan Tim Tanggap Darurat Komputer India (CERT-In), AWS diperlukan untuk mengumpulkan dan memvalidasi informasi identitas Anda sebelum memberi Anda akses baru atau lanjutan ke AWS layanan. Identitas Anda harus diverifikasi menggunakan nama dari tagihan India atau alamat kontak yang Anda berikan. Selama verifikasi, AWS akan memeriksa apakah nomor dokumen valid dan apakah nama yang Anda berikan cocok dengan nama yang terkait dengan dokumen yang Anda gunakan untuk verifikasi pelanggan. Nama yang Anda pilih antara kontak atau informasi penagihan harus sama persis dengan nama yang muncul pada dokumen.

Untuk memperbarui nama dan alamat penagihan, lihat halaman [Preferensi pembayaran](#). Untuk memperbarui nama dan alamat kontak Anda, lihat [the section called “Perbarui kontak utama untuk Anda Akun AWS”](#). Jika Anda mengedit informasi apa pun yang sebelumnya Anda gunakan untuk verifikasi pelanggan, seperti nama atau India-based alamat dari informasi penagihan atau kontak Anda, Anda mungkin perlu memperbarui dan mengirimkan kembali informasi verifikasi pelanggan Anda.

Periksa status verifikasi pelanggan Anda

Anda dapat melihat status verifikasi pelanggan Anda kapan saja di halaman verifikasi Pelanggan. Jika status verifikasi Anda diperlukan Verifikasi atau Verifikasi gagal, buat atau perbarui informasi verifikasi pelanggan Anda dan kirimkan untuk verifikasi.

Buat informasi verifikasi pelanggan Anda

Untuk menyelesaikan verifikasi pelanggan, Anda harus memberikan informasi dari dokumen India yang diterima. Untuk daftar jenis dokumen yang diterima, lihat [the section called “Dokumen India yang diterima untuk verifikasi pelanggan”](#).

1. Masuk ke [Konsol Manajemen AWS](#).
2. Pada bilah navigasi, di sudut kanan atas, pilih nama akun Anda (atau alias), lalu pilih Akun.
3. Di bawah Pengaturan lain, pilih Verifikasi pelanggan.

Jika Anda belum memberikan informasi verifikasi pelanggan Anda sebelumnya, Anda akan melihat halaman Buat verifikasi pelanggan.

4. Pilih nama yang sama persis dengan nama pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen.
5. Berikan informasi yang tersisa yang diminta di halaman. Bergantung pada jenis dokumen yang Anda pilih, Anda mungkin perlu mengunggah salinan bagian depan dan belakang dokumen. Jika Anda mengunggah file gambar, pastikan semua informasi dalam dokumen terlihat dan terbaca.
6. Pilih Kirim.

Anda akan diberitahu tentang hasil verifikasi pelanggan dan langkah selanjutnya melalui email atau di Dasbor AWS Kesehatan.

Mengedit informasi verifikasi pelanggan Anda

Anda dapat mengedit informasi verifikasi pelanggan Anda, seperti tujuan utama pendaftaran akun, jenis organisasi Anda, dan nama, jenis dokumen, unggahan dokumen, atau informasi dokumen yang ingin Anda gunakan untuk verifikasi.

Jika Anda mengedit nama atau jenis dokumen yang akan digunakan untuk verifikasi pelanggan, atau memperbarui informasi dokumen apa pun, menyimpan perubahan akan mengharuskan identitas Anda diverifikasi lagi.

1. Masuk ke [Konsol Manajemen AWS](#).
2. Pada bilah navigasi, di sudut kanan atas, pilih nama akun Anda (atau alias), lalu pilih Akun.
3. Di bawah Pengaturan lain, pilih Verifikasi pelanggan.
4. Pilih Edit, lalu perbarui informasi yang ingin Anda ubah.

Saat Anda memperbarui informasi, perhatikan panduan berikut:

- Jika Anda memilih nama yang berbeda, nama harus sama persis dengan nama pada dokumen yang Anda rencanakan untuk digunakan untuk verifikasi pelanggan. Misalnya, jika Anda berencana untuk memverifikasi akun bisnis menggunakan Sertifikat Pendirian, Anda harus memberikan nama bisnis yang muncul pada dokumen.

- Jika Anda memilih jenis dokumen yang berbeda, Anda perlu mengunggah salinan bagian depan dan belakang (jika ada) dokumen. Semua informasi dalam unggahan dokumen harus terlihat dan terbaca.
- Jika Anda memiliki akun pribadi dan berencana untuk menggunakan SIM yang tidak dikeluarkan oleh Uni India, sebaiknya gunakan jenis dokumen pribadi yang berbeda untuk verifikasi.

Untuk daftar jenis dokumen yang diterima, lihat [the section called “Dokumen India yang diterima untuk verifikasi pelanggan”](#).

5. Pilih Kirim.

Jika identitas Anda harus diverifikasi lagi karena jenis perubahan yang Anda simpan, Anda akan diberitahu tentang hasil verifikasi pelanggan dan langkah selanjutnya melalui email. Anda juga dapat melihat hasilnya dengan kembali ke halaman verifikasi Pelanggan atau di Dasbor AWS Kesehatan.

Dokumen India yang diterima untuk verifikasi pelanggan

Jenis dokumen berikut yang dikeluarkan oleh pemerintah India diterima untuk verifikasi pelanggan.

Note

Tautan yang dibagikan di bawah ini dapat berubah oleh pemerintah.

- Kartu PAN - Tersedia dalam format digital dan fisik, kartu Nomor Rekening Permanen (PAN) berisi pengidentifikasi alfanumerik unik yang dikeluarkan oleh Departemen Pajak Penghasilan India untuk individu, perusahaan, dan entitas. PAN terdiri dari sepuluh karakter, termasuk huruf dan angka, dalam format **AAAAA1111A**. Untuk menggunakan dokumen ini untuk verifikasi, Anda juga harus memberikan tanggal lahir (individu) atau tanggal pendirian (bisnis) yang muncul pada dokumen PAN dan mengunggah sisi depan kartu. Anda dapat mengunjungi [situs web resmi Departemen Pajak Penghasilan](#) untuk memeriksa validitas PAN Anda.
- ID Pemilih Card/EPIC - Kartu ID pemilih, juga dikenal sebagai Kartu Identitas Foto Pemilih (EPIC), berisi nomor identifikasi unik yang dikeluarkan oleh Komisi Pemilihan India untuk pemilih yang memenuhi syarat di India. ID/EPIC Nomor pemilih terdiri dari sepuluh karakter, termasuk huruf dan angka. Anda dapat mengunjungi situs resmi [Komisi Pemilihan India](#) untuk memeriksa validitas

ID pemilih Anda. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus mengunggah sisi depan dan belakang kartu.

- Surat Izin Mengemudi - Jika SIM Anda tidak dikeluarkan oleh Uni India, kami sarankan menggunakan jenis dokumen yang berbeda untuk verifikasi. Nomor SIM terdiri dari 12-16 karakter, termasuk huruf, angka, dan spasi atau tanda hubung. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus memberikan tanggal lahir Anda dan mengunggah sisi depan dan belakang kartu. Anda dapat pergi ke [situs Sewa Parivahan](#) Kementerian Transportasi Jalan dan Jalan Raya untuk memeriksa validitas SIM Anda.
- Sertifikat Pendirian - Sertifikat pendirian adalah dokumen yang dikeluarkan oleh Kementerian Urusan Korporat (MCA) yang memberi tanggal pendaftaran bisnis sebagai badan hukum. Sertifikat ini digunakan untuk mengidentifikasi dan melacak perusahaan yang terdaftar di India secara unik. Setiap sertifikat berisi Corporate Identification Number (CIN), yang merupakan pengidentifikasi alfanumerik unik yang terdiri dari 21 karakter, termasuk huruf dan angka. Untuk menggunakan dokumen ini untuk verifikasi, Anda harus mengunggah sertifikat dokumen pendirian. Anda dapat pergi ke [portal Kementerian Urusan Korporat](#) untuk memeriksa validitas CIN Anda.

Jenis dokumen India yang berbeda diterima untuk akun pribadi dan bisnis:

- Untuk akun pribadi - kartu PAN, ID pemilih card/EPIC, dan SIM.
- Untuk akun bisnis - kartu PAN dan sertifikat pendirian.

Kelola Anda AWS Akun India

Kecuali untuk tugas-tugas berikut, prosedur untuk mengelola akun Anda sama dengan akun yang dibuat di luar India. Untuk informasi umum tentang mengelola akun Anda, lihat [Konfigurasi akun Anda](#).

Gunakan Konsol Manajemen AWS untuk melakukan tugas-tugas berikut:

- [Menambahkan atau mengedit Nomor Rekening Permanen](#)
- [Mengedit beberapa Nomor Akun Permanen](#)
- [the section called “Kelola informasi verifikasi pelanggan Anda”](#)
- [Edit beberapa Nomor Pajak Barang dan Jasa \(GST\)](#)
- [Lihat faktur pajak](#)

Riwayat dokumen untuk Panduan Pengguna Manajemen Akun

Tabel berikut menjelaskan rilis dokumentasi untuk Manajemen AWS Akun.

Perubahan	Deskripsi	Tanggal
Nama akun baru APIs	Support untuk yang baru GetAccountInformation , dan PutAccountName APIs untuk melihat atau memodifikasi nama akun.	April 22, 2025
Akhir dukungan untuk mengedit pertanyaan tantangan keamanan	Menghapus topik Edit pertanyaan tantangan keamanan Anda dari panduan karena dukungan telah berakhir.	Januari 6, 2025
Email utama baru APIs	Support untuk yang baru GetPrimaryEmailStartPrimaryEmailUpdate , dan AcceptPrimaryEmailUpdate APIs untuk memperbarui alamat email pengguna root alamat email secara terpusat untuk akun anggota mana pun. AWS Organizations Untuk informasi selengkapnya, lihat Memperbarui alamat email pengguna root untuk akun anggota di Panduan AWS Organizations Pengguna.	Juni 6, 2024

Menulis ulang topik akun tutup	Sepenuhnya merombak seluruh topik akun penutupan termasuk menambahkan langkah-langkah untuk cara menutup akun anggota dan manajemen.	Februari 1, 2024
Akhir dukungan untuk menambahkan pertanyaan tantangan keamanan baru	Menambahkan konten baru yang mencatat bahwa opsi untuk menambahkan pertanyaan tantangan baru telah dihapus dari halaman Akun.	Januari 5, 2024
Akhir dukungan untuk aws-portal namespace	AWS Identity and Access Management (IAM) tindakan yang sebelumnya digunakan untuk mengelola akun Anda (misalnya, <code>aws-portal:ModifyAccount</code> dan <code>aws-portal:ViewAccount</code>) telah mencapai akhir dukungan standar.	Januari 1, 2024
Menulis ulang topik Daerah	Merombak seluruh topik Wilayah sepenuhnya termasuk menambahkan kontrol perluas dan ciutkan.	Oktober 8, 2023
Memindahkan topik pengguna root ke Panduan Pengguna IAM	Diskusi konsolidasi tentang pengguna root ke dalam satu topik, menambahkan tautan referensi silang ke topik pengguna root yang dipindahkan ke Panduan Pengguna IAM.	18 September 2023

Bagian baru ditambahkan ke topik kontak akun utama	Menambahkan nomor Telepon baru dan bagian persyaratan alamat email.	12 September 2023
Informasi kontak baru APIs	Support untuk yang baru GetContactInformation dan PutContactInformation APIs.	22 Juli 2022
AWS Manajemen Akun sekarang mendukung pembaruan kontak alternatif melalui AWS Organizations konsol.	Sekarang Anda dapat memperbarui kontak alternatif organisasi Anda melalui AWS Organizations konsol menggunakan izin API Akun yang disediakan oleh kebijakan AWS Organizations terkelola yang diperbarui.	8 Februari 2022
Rilis awal	Rilis awal Panduan Referensi Manajemen AWS Akun	30 September 2021

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.